VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Rámec pro testování blockchain technologie

Framework for Testing Blockchain Technology Implementations

2020 Bc. Miloslav Szczypka

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Zadání diplomové práce

Student: **Bc. Miloslav Szczypka**

Studijní program: N2647 Informační a komunikační technologie

Studijní obor: 1801T064 Informační a komunikační bezpečnost

Téma: Rámec pro testování blockchain technologie
Framework for Testing Blockchain Technology Implementations

Jazyk vypracování: čeština

Zásady pro vypracování:

Práce je zaměřena na tvorbu vlastní implementace blockchain technologie. Student provede rešerši aktuálně používaných implementací blockchain technologie a v teoretické části tyto implementace porovná. Na základě zjištěných faktů provede návrh a implementaci vlastní kryptoměny, která bude navržena jako testovací rámec pro budoucí experimenty. Mezi takové experimenty může patřit výkonnostní testování šifrovacích algoritmů, algorimů pro vyhledání uzlů v síti a jiné. Funkčnost řešení student prokáže provedením studentem vybraných experimentů.

Hlavní body zadání:
1. Rešerše aktuálního stavu na poli implementací blockchain technologie.
2. Návrh a implementace vlastní verze blockchain technologie.
3. Návrh dvou netriviálních experimentů, které prověří funkčnost řešení.
4. Vyhodnocení experimentu a prezentace výsledků.

Seznam doporučené odborné literatury:

[1] Andreas M. Antonopoulos, Mastering Bitcoin: Programming the Open Blockchain 2nd Edition, O'Reilly Media, 2017, ISBN: 978-1491954386
[2] Jimmy Song, Programming Bitcoin: Learn How to Program Bitcoin from Scratch, O'Reilly Media, 2019, ISBN: 978-1492031499

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **Ing. Jan Plucar, Ph.D.**

Datum zadání: 01.09.2019

Datum odevzdání: 30.04.2020

doc. Ing. Jan Platoš, Ph.D.
vedoucí katedry

prof. Ing. Pavel Brandštetter, CSc.
děkan fakulty

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

V Ostravě 15. května 2020 .....

Souhlasím se zveřejněním této diplomové práce dle požadavků čl. 26, odst. 9 Studijního a zkušebního řádu pro studium v magisterských programech VŠB-TU Ostrava.

V Ostravě 15. května 2020 .....

Rád bych na tomto místě poděkoval všem, kteří mi s prací pomohli, protože bez nich by tato práce nevznikla.

Abstrakt

Blockchain je technologie, která může zásadně změnit způsob provádění finančních transakcí, ale také způsob ověření pravosti dokumentů nebo také důvěryhodnost voleb. V dnešním světě se tato technologie stále více skloňuje a je jisté, že ještě o ní hodně uslyšíme. Většina lidí zná momentálně blockchain pouze ve spojitosti s kryptoměnami, ale již v dnešní době se tato technologie používá i v bankovnictví, ve státní sféře či pojišťovnách. Cílem této práce je ukázat jak blockchain funguje, ukázat možnosti jeho využití, ale také jeho slabiny.

Klíčová slova: blockchain, Bitcoin, Kryptoměny

Abstract

Blockchain is a technology that can fundamentally change the way financial transactions are made, but also the way documents are authenticated or the credibility of choices. In today's world, this technology is becoming increasingly inflexible, and it is certain that we will hear a lot about it. Most people currently know blockchain only in connection with cryptocurrencies, but nowadays this technology is also used in banking, in the state sphere or in insurance companies. The aim of this work is to show how blockchain works, show possibilities of its use, but also its weaknesses.

Keywords: blockchain, Bitcoin, Cryptocurrencies

Obsah

Seznam použitých zkratek a symbolů **10**

Seznam obrázků **11**

Seznam tabulek **12**

1 Úvod **13**

2 Aktuální výzkum **14**

3 Blockchain **19**

3.1 Motivace . . . 19
3.2 Historie . . . 19
3.3 Kryptografie . . . 22
3.4 Části blockchainu . . . 24
3.5 Jak blockchain funguje? . . . 30
3.6 Slabiny a problémy blockchainu . . . 36
3.7 Distribuované souborové systémy . . . 40
3.8 Alternativa k blockchainu . . . 42

4 Možnosti využití Blockchainu **46**

4.1 Finanční sektor . . . 46
4.2 Státní orgány . . . 46
4.3 Školství . . . 46
4.4 Shrnutí . . . 47

5 Vybrané Blockchainové projekty **48**

5.1 Kryptoměny . . . 48
5.2 Stabilní měny založené na blockchainu . . . 52
5.3 Blockchainové knihovny . . . 53

6 Vlastní implementace **55**

6.1 Proč vlastní implementace . . . 55
6.2 Možnosti využití . . . 55
6.3 Návrh . . . 55
6.4 Funkčnost . . . 58

7 Otestování funkčnosti a experimenty s VSB Coin **62**
7.1 Testovací síť 62
7.2 Spuštění testovací sítě 62
7.3 Příprava konfigurací pro testování 65
7.4 Testování 67

8 Závěr **71**

Literatura **72**

Přílohy **74**

Seznam použitých zkratek a symbolů

TPS	–	Transactions Per Second
VSCC	–	Validation System Chaincode
vCPU	–	virtual Central Processing Unit
IoT	–	Internet of Things
HW	–	Hardware
SSD	–	Solid State Disk
P2P	–	Peer to Peer
Dapps	–	Decentralized applications
SPV	–	Simplified Payment Verification
ASIC	–	Application Specific Integrated Circuit
DNS	–	Domain Name System

Seznam obrázků

1 Ukázka jak počet vCPU ovlivňuje TPS [3] . . . 15
2 Ukázka výsledku srovnání daných implementací [4] . . . 15
3 Porovnání rychlost blockchainu a Databáze [7] . . . 18
4 blockchain . . . 20
5 Srovnání centralizované a dencetralizované sitě . . . 20
6 Hlavní myšlenka blockchain 1.0 . . . 21
7 Digitální podpis . . . 24
8 Ukázka Hardforku . . . 25
9 Blockchainová síť . . . 27
10 Merkle Tree . . . 29
11 Genesis blok Bitcoinu . . . 31
12 Propojení bloků . . . 33
13 Útok Eclipse . . . 38
14 Ukázka 51% útoku . . . 40
15 Hashgraph . . . 43
16 Tangle . . . 44
17 TOP 10 kryptoměn k 10.5.2020 . . . 49
18 Graf ceny LTC . . . 50
19 VirtualBox testovací síť . . . 63
20 Snímek obrazovky plného uzlu . . . 64
21 Snímek obrazovky plného uzlu při odeslání transakce . . . 64
22 Snímek obrazovky těžebního uzlu po obdržení transakce . . . 65
23 Srovnání rychlostí hešovacích funkcí . . . 68
24 Konfigurace s 10 transakcemi v bloku . . . 69
25 Konfigurace s 25 transakcemi v bloku . . . 69
26 Konfigurace s 50 transakcemi v bloku . . . 70

Seznam tabulek

1 Srovnání vybraných blockchainových projektů k 28.4.2020 52
2 Rostoucí složitost 66
3 Konstantní složitost 66
4 Nastavení konfiguraci 66
5 Pravidla pro generování transakci 66
6 Výběr z výstupního souboru bloků 67
7 Výběr z výstupního souboru transakcí 67
8 Srovnání rychlostí hešovacích funkcí. Hodnoty jsou uvedeny v sekundách 68

1 Úvod

Dnešní doba je plná nových nadějných technologií a právě blockchain patří mezi jednu z nich. Blockchainová technologie se nejčastěji spojuje s kryptoměnami a to především s kryptoměnou Bitcoin, která je průkopníkem v oblasti kryptoměn. Myšlenka blockchainu je taková, že databázi nespravuje jedna autorita, ale databáze je distribuována mezi uživatele a každý si může transakce ověřit. Díky tomuto Kryptoměny získaly značně na popuplaritě a jejich hodnota raketově vyrostla. Není zde žádná centrální banka a nikdo vám nemůže vaše kryptoměny blokovat či jinak omezovat. Další výhodou je fakt, že transakce jsou zpracovány poměrně rychle a to i bez ohledu na jejich hodnotu a jako bonus je za ně také poměrně nízký poplatek.

Na začátku této práce ukážu, jakými způsoby se dnes dají porovnávat jednotlivé implementace blockchainu a pokusím se je shrnout. Následně detailně popíši jak blockchain funguje, z čeho se skládá a co vše s ním lze provádět. Popíši také problémy, které v blockchainu mohou nastat, nebo kde se nachází jeho zranitelnosti. Pokusím se srovat použití blockchainu oproti konvenčním metodám a vysvětlím jeho výhody a nevýhody vůči nim.

Následně vytvořím vlastní implementaci blockchainu a popíši ji. Implementaci chci udělat modulární a flexibilní, hlavně z důvodu toho, abych mohl následně lehce porovnávat různé metody v rámci blockchainu. Implementaci blockchainu budu psát v programovacím jazyku Python.

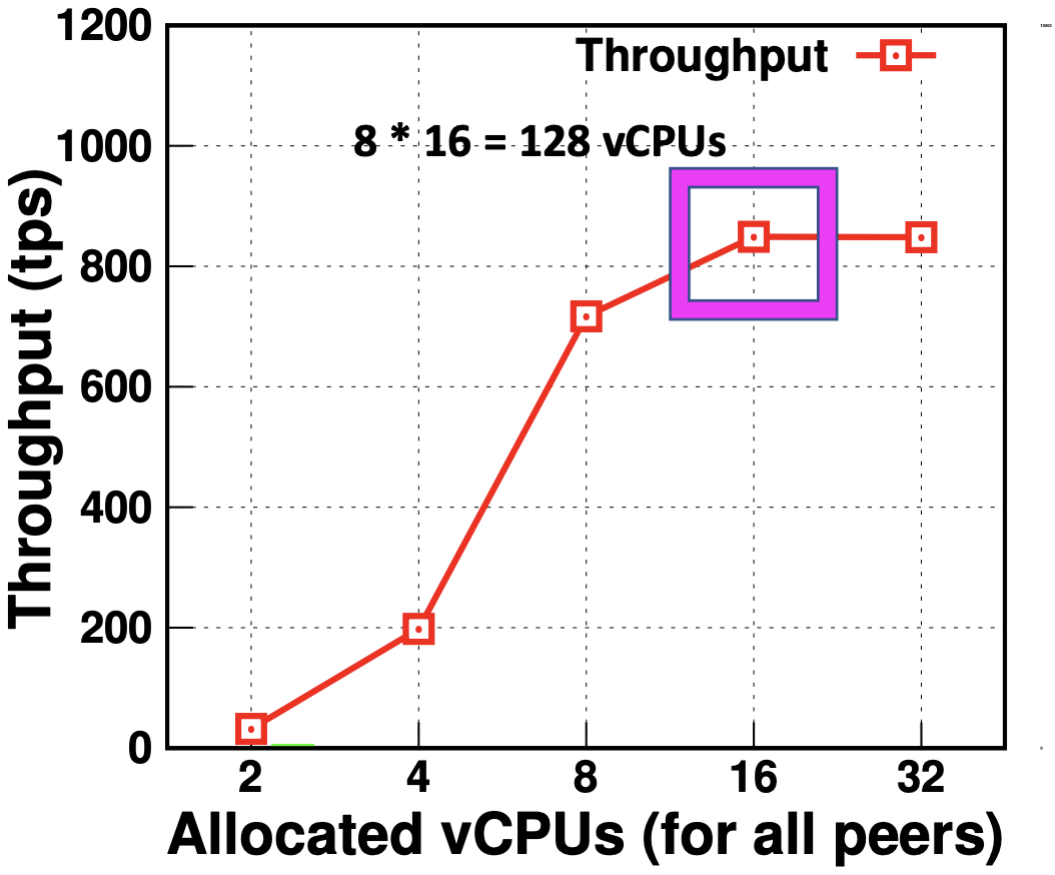
Cílem této práce by měl být jakýsi framework, který umožní použití různých implementací blockchainu. Tento framework posléze půjde využít na různé projekty, které budou založeny na blockchainu. Můžeme ho také využít k porozumění jak blockchain funguje, studovat jak se chová či testovat jeho slabiny.

2 Aktuální výzkum

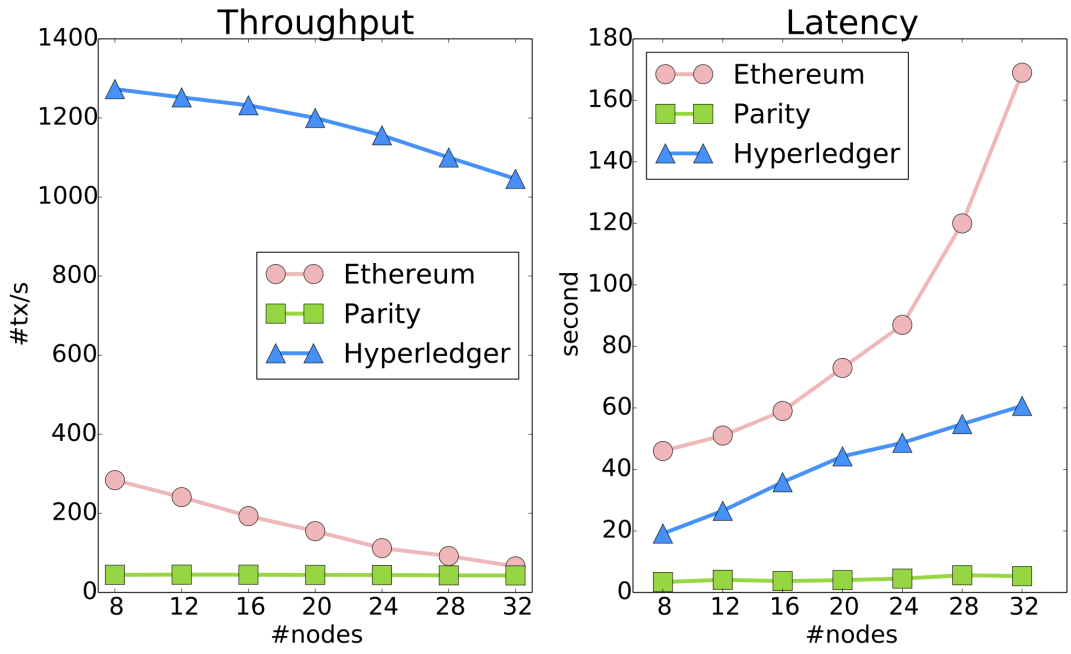
Aktuální situace v oblasti tvorby blockchainových technologií je velmi dynamická a mění se doslova každým dnem. Komunita nadšenců, soukromé společnosti či vládní organizace napříč světem začínají stále častěji s touto technologií experimentovat. Nejčastěji se blockchain využívá pro tvorbu digitální měny. Těchto digitálních měn již existuje několik tisíc a jako etalon se považuje Bitcoin[1]. Avšak je zde jedna otázka, jak určit, která je nejlepší a podle čeho můžeme vůbec měny srovnávat. Jednotlivé digitální měny můžeme srovnávat podle maximálního počtu transakcí za sekundu, označovány jako TPS. Transakce za sekundu jsou důležité v mnoha oblastech. Například logistika a e-commerce je založena na okamžitém ověření transakce a následném odeslání zboží. Ale tento benchmark nám také může říct, pro kolik lidí je tato digitální měna schopna zpracovávat transakce v rozumném čase. Projekt QtumX[2] vytvořil kryptoměnu, která je unikátní v několika směrech. Tento projekt je zaměřen právě na počet transakcí za sekundu a srovnání jejich implementací s Bitcoinem, který má údajně 7 TPS, kdežto QtumX má 10000 TPS. Pro porovnání je také vedeno, že zprostředkovatel plateb VISA má 27000 TPS. Rychlost zpracování transakcí však ovlivňuje řada parametrů blockchainu.

To, jak zvolit různé parametry blockchainu, či jaké použít algoritmy a podobně, je také nemalý problém a zároveň i výzva. Důvodem je to, žemomentálně neexistuje žádný jednotný přístup. Této problematice se věnovalo několik práci, a mě zaujala práce[3], která zkoumala platformu Hyperledger Fabric. Testování spočívalo ve změně nastavitelných parametrů jako je například velikost bloku, schvalovací pravidla nebo alokace zdrojů. Výsledkem této práce je jakýsi návod na nastavení těchto parametrů, které byly později v projektu Hyperledger Fabric implementovány. Výkonnost této platformy byla posuzována podle několika typů prodlev. Jednou z nich je prodleva vysílání, která spočívá v časovém intervalu od odeslání požadavku odesílatele až po potvrzení požadavku příjemcem. Druhou prodlevou je čas, který uzel v síti potřebuje pro ověření transakce a jejího provedení. Tato práce pak definovala různé prodlevy na úrovních bloků. Jednou z nich je VSCC prodleva, která měří čas ověření všech transakcí v bloku. Druhou takto definovanou prodlevou je prodleva aktualizace databáze, která měří dobu zápisu všech ověřených transakcí do blockchainu. Pokusy se prováděly ve virtuálním prostředí a to umožnilo otestovat, jak počet procesorů přidělených každému uzlu ovlivňuje rychlost zpracování transakce v celé síti. Z grafu na obrázku 1 lze vidět, že neustálé přidávání virtuálních procesorů nevede ke stálému zvyšování zpracovaných transakcí v síti, neboť pravděpodobně již naráží na limit jiné součásti uzlu nebo sítě.

V další práci[4] z roku 2017 byl navrhnut první ucelený benchmarkovací nástroj BlockBench pro testování výkonnosti soukromých blockchainových systémů. Z tohoto faktu plyne, že testování výkonnosti blockchainových aplikací je poměrně nová věc, která zatím není moc rozšířena. Tento nástroj obsahuje metriky pro hodnocení výkonnosti zpracování dat a nástroje pro porozumění výkonnosti na různých úrovních. Následně byla provedena analýza třech hlavních blochchainových systémů: Ethereum, Parity a Hyperledger. Výsledek těchto analýz ukázal, že



Obrázek 1: Ukázka jak počet vCPU ovlivňuje TPS [3]



Obrázek 2: Ukázka výsledku srovnání daných implementací [4]

současné blockchainy nejsou stavěné na rozsáhlé zpracovávání dat. BlockBench provádí makro a mikro benchmarky. Rozdíl mezi těmito typy je ten, že makro benchmark se zabývá obecnými statistikami, jako je propustnost systému, škálovatelnost nebo bezpečnost. Mikro benchmark se zabývá výkonností různých částí blockchainového systému jako je například využití disku. Obrázek 2 představuje srovnání daných implementací blockchainu, jinými slovy vlevo propustnost sítě vzhledem k počtu uzlů a vpravo odezvu vzhledem k počtu uzlů. Lze vidět, že rostoucí počet uzlů způsobuje zpomalení sítě jak s ohledem na propustnost, tak také na odezvu sítě.

Další práce[5], která mě zaujala, zkoumala výkonnost blockchainové platformy Quorum. Quorum je open source blockchainová platforma, založená na Ethereum[6]. Práce dospěla k tomu, že nejmenší prodleva zpracovávání transakcí je při čtení. Zásadně větší prodleva je u zapisování transakcí, která je závislá na velikosti bloku. Dále se přišlo na to, že soukromé transakce více zatěžují systém a snižují propustnost sítě kvůli šifrování a dešifrování, ale také kvůli navazování bezpečného spojení mezi uzly. Maximální propustnosti bylo dosaženo při 900 TPS, avšak systém si nevedl dobře při dosahování koncesa, jakým blokem řetěz pokračuje. Mikro testování platformy ukázalo, že prodleva transakcí se zvyšuje při velkém počtu čtení a zápisů ve smart kontraktech. Naopak velikost dat zde nemá skoro žádný dopad na prodlevu transakcí.

Jiný článek[7] opět zmiňuje, že testování výkonnosti blockchainových aplikací je zatím teprve na začátku. Snahy o měření výkonnosti takových systémů nejsou většinou standardizovány a jsou spíše proprietární. Práce také popisuje, které aspekty se týkají testování výkonnosti. Mezi takové vlastnosti se řadí testování funkcionality, kdy je například žádoucí testovat smart kontrakty před tím, než se začnou používat v transakcích. Další důležitou oblastí testování blochchainových systémů je testování samotného systému, přičemž je kladen důraz na testování odolnosti proti výpadkům v síti, testování kompatibility připojení různých klientů nebo testování latence a fungování při omezené rychlosti připojení. Co se týče samotné výkonnosti blockchainových systémů, práce hovoří o propustnosti transakcí, latenci transakcí, odolnosti vůči chybám nebo škálovatelnosti.

Velmi zajímavá publikace[8] porovnávala výkonnost blockchainu oproti klasickým relačním databázím hlavně z pohledu rychlosti čtení a zápisů. Závěrem této práce z roku 2018 je fakt, že v současné době nemůže být vytvořen obchodní systém čistě na technologii blockchainu tak, jak ho známe dnes. Důvodem je nízká rychlost čtení a zápisů. Tento fakt lze vidět ve srovnání na obrázku 3, kde test běžel na shodném HW s SSD diskem. Řešení by mohlo spočívat v kombinaci blockchainu a relační databáze. Tato práce dokonce navrhla metody, jak začlenit blockchain do IoT přístrojů, které jsou výrazné svou minimalističností. Kombinací blockchainu a relační databáze v rámci testovacích dat se podařilo zmírnit limity výkonnosti blockchain technologie.

Některé práce hovoří i o výkonové náročnosti na síť i výkon stroje, na kterém běží systém založený na blockchainu. Pro vývojáře takových systémů to znamená, že při testování výkonnosti musí implementovat logiku událostí takového systému a použít simulátor nebo nasadit takový systém na fyzické počítače a spustit zátěžový test. Cílem této práce[9] bylo vytvořit testovací prostředí pro systém na bázi blockchainu ve virtuálním prostředí. Výhodou takového prostředí je

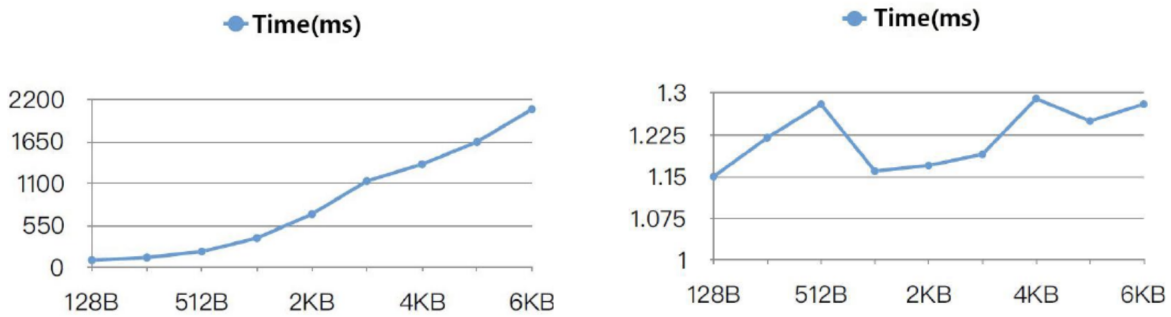
jednoduché nasazení či nízká nákladnost. Nevyhnutelnou nevýhodou je však zpoždění provádění instrukcí. V některých případech je zpoždění tak vysoké, že nelze navázat TCP spojení, což je hlavní limitace virtuálního prostředí.

Další práce [10] vytvořila implementaci blockchainu pro průmyslové IoT systémy. Jeho předností je dynamická změna hashovacího algoritmu v závilosti na počtu posílaných transakcí v síti. Tímto se vylepšil výkon sítě a hlavně jeho propustnost. Jejich simulace ukázaly, že navrhnutá implementace je vhodná pro oblasti, kde je nutné vyřídit transakce v co nejrychlejším čase. Dále autoři odhalili, že pokud jsou hašovací funkce prováděny ve vláknech nebo se použijí nenáročné hašovací funkce, je tento systém vhodní i do IoT oblasti.

Následující práce [11] nasadila laťku ještě o něco výše a snaží se o vytvoření bezpečného blockchainu pro IoT s využitím ve zdravotnictví. Tato práce navrhla řešení, které vylepšují stránku bezpečnosti v IoT pomocí blockchainu, soukromých a veřejných klíčů a mnoha dalších výpočetně nenáročných kryptografických funkcí. Tímto dali možnost vytvoření postupu k řízení přístupu k lékařským záznamům. Autoři se také zabývají snížením závažnosti DoS útokú na sytémy podobné tomu, který navrhli v této práci. Tento projekt je však v testovací fázi a není zatím komerčně využíván.

Tento článek [12] dokazuje fakt, že se nachází stále nové a nové oblasti využití aplikací založených na blockchainu. Konkrétně se autoři tohoto článku zabývali použitím blockchainu v oblasti energetiky a objevili několik případů využití blockchainu jako například decentralizované obchodování s energií, nebo správa energetické sítě založená na blockchainu. Práce také uvádí, že většina projektů, které se zabývají aplikací blockchainu na energetický sektor jsou zatím ve fázi vývoje. Zároveň také stále probíhá výzkum pro zlepšení škálovatelnosti a bezpečnosti těchto aplikací.

Jako poslední bych v této části práce zmíňil práci[13], která se na problematiku blockchainu dívá trochu jinak. Na začátku porovnává veřejný blockchain s privátním a následně spouští zátěžové testy. Tato práce odhalila, že pokud obětujeme decentralizovanost a vytvoříme autority a důvěru mimo síť, tak se podstatně zvýší výkonnost a škálovatelnost celého systému. Avšak nabízí se nám zde otázka, zda jsou to lidé schopni akceptovat, jelikož soukromý blockchain nepotřebuje výpočetní výkon k ověřování důvěry jako u veřejných blockchainů. Dále se v této práci objevilo, že platforma Hyperledger Fabric je mnohem rychlejší a škálovatelnější než Bitcoin i Ethereum a to i v ohledu propustnosti sítě. Další otázkou však zůstává, zda je dostatečně dobrý natolik, aby nahradil dnes používané centralizované systémy.



(a) Rychlost čtení/zápisu v blockchainu s 8 uzly

(b) Rychlost čtení/zápisu v relační databázi

Obrázek 3: Porovnání rychlost blockchainu a Databáze [7]

3 Blockchain

V této kapitole popíši doposud zmiňovaný blockchain, z čeho se skládá a jak funguje. Blockchain lze chápat jako distribuovanou databázi s funkcionalitou navíc, přičemž málokdo ví, že blockchain je vlastně velmi jednoduchý. Dá se říci, že blockchain je jednoduše řetěz bloků, tuto skutečnost popisuje obrázek 4, ve kterých jsou uloženy transakce a poté jsou navzájem provázány a následně distribuovány mezi jednotlivé uzly v síti. Bloky jsou vzájemně provázany, respektivě každý nový blok využívá informaci z předchozí a takovým způsobem to pokračuje až k prvnímu bloku. Kvůli jeho transparentnosti a neměnnosti bývá blockchain nazýván jako "protokol pravdy".

3.1 Motivace

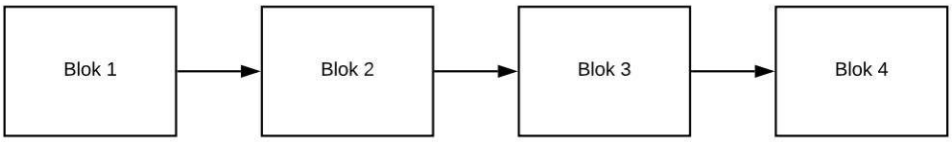
Motivací pro vznik blockchainu je především svoboda, díky neexistenci centrální autority, ale také bezpečnost, kterou se blockchain snaží dosáhnout kryptografií a neměnností dat, které byly do něho zapsány. K tomu, aby blockchain dosáhl těchto požadovaných vlastností, distribuuje informace mezi všechny uživatele systému. Žadné transakce se neupravují, ale vždy vzniká nová, která může na jinou navazovat, tudíž můžeme sledovat všechny transakce, které byly provedeny s danou digitální měnou. Díky tomu, že informace jsou distribuovány mezi všechny uživatele daného systému, je systém nejen transparetní, ale také odolný vůči výpadkům části uzlů. Orázek 5 ukazuje srovnání decentralizovaného systému se systémem s centrálním prvkem. V blockchainu si každý může prohlížet libovolné transakce, protože tato data jsou dostupná každému. Tato skutečnost je zapříčiněna tím, že zde neexistuje žádný centrální prvek, který by tato data uchovaval v tajnosti. Díky decentralizaci se uživatelé nemusí bát, že by je někdo mohl jednoduše odříznout od systému, nebo by někdo vymazal či upravil některé jejich transakce.

3.2 Historie

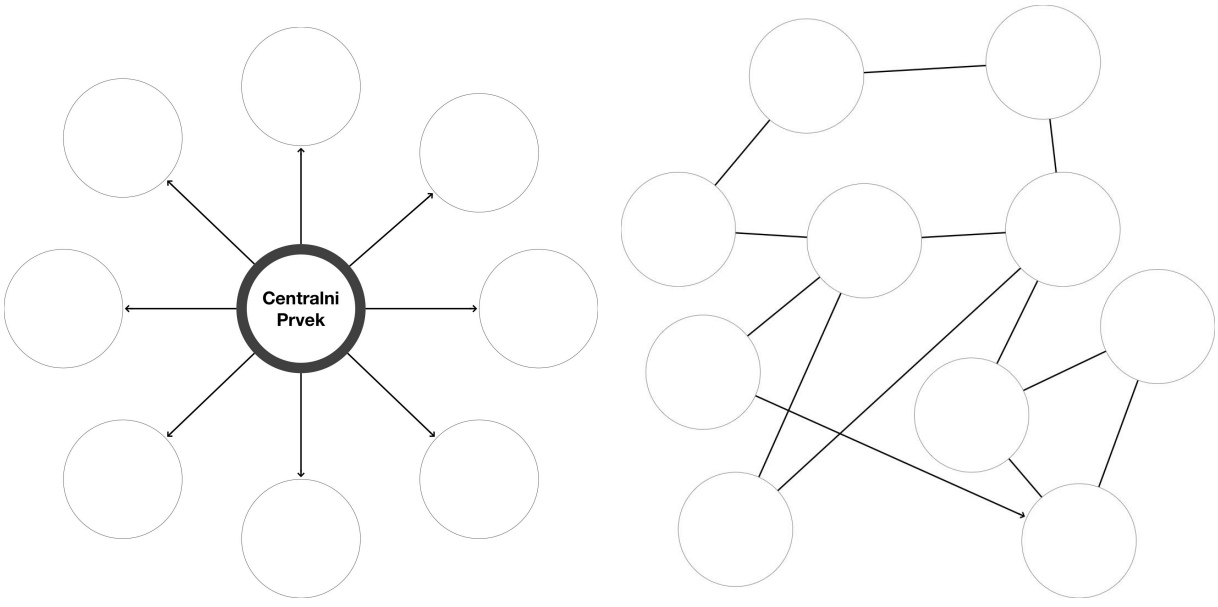
První myšlenka technologie, kterou lze považovat za blockchain, pochází již z roku 1991, kdy Stuart Haber a W. Scott Stornetta v práci[14] popsali systém, který zamezoval manipulovat s časovými razítky dokumentů a to právě pomocí kryptografického zabezpečení řetězce bloků. Následující rok byl tento systém vylepšen přidáním Merkle stromů, což umožnilo v jednom bloku ověřit více dokumentů. Bohužel se tento systém neujal a až v roce 2008, kdy skupina či programátor známý jako Satoshi Nakamoto publikoval článek[1], který popsal blockchain jako elektronický platební P2P systém zvaný Bitcoin.

3.2.1 Blockchain 1.0

Za blockchain verzi 1.0 je považována aplikace blockchainu jako alternativního platebního prostředku bez centrální autority, který je také nezmanipulovatelný a transparetní. Pro představu konkrétního využití blockchain 1.0 si můžeme představit prvotní verzi Bitcoinu, který využívá

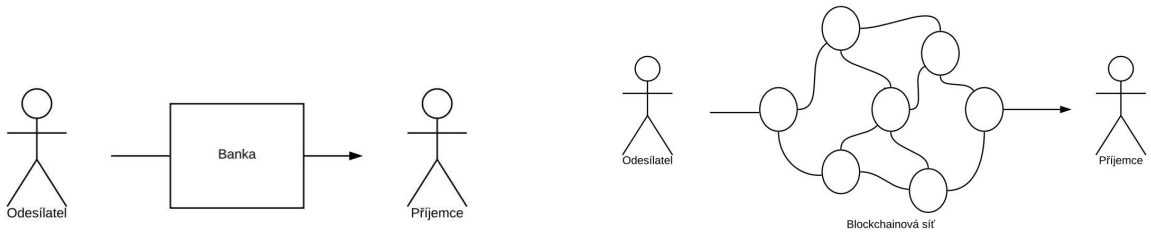


Obrázek 4: blockchain



(a) Síť s centrálním prvkem (b) Decentralizovaná síť

Obrázek 5: Srovnání centralizované a dencetralizované sitě



(a) Odesílání transakce skrz banku

(b) Odesílání transakce skrz blockchain

Obrázek 6: Hlavní myšlenka blockchain 1.0

blockchain jako distribuovanou účetní knihu. První generace blockchainu je postavena na 3 vrstvách:

- Token kryptoměny - Název dané měny (BTC, LTC, atd.)
- Protokolová vrstva - Obsahuje protokoly dané kryptoměny, ale také pravidla jak se bude systém chovat (Např., způsob zpracování transakce)
- Základ celé platformy - blockchain - Decentralizována účetní kniha

Tyto 3 vrstvy představují jakýsi základní stavební kámen každé kryptoměny. Kryptoměny mohou mimojiné využívat i tzv. sdílený blockchain, tedy blockchain jiné kryptoměny.

Obecně můžeme říci, že blockchain 1.0 slouží k P2P platbám bez zásahu centrální autority (Obrázek 6), tedy digitálním měnám či kryptoměnám.

3.2.2 Blockchain 2.0

Druhá generace blockchainu vychází z verze 1.0, ale je obohacena o chytré kontrakty. Jsou to doslova malé programy, které jsou zapsány v blockchainu a umožňují automaticky provádět předem nastavené instrukce a podmínky. Díky tomuto vylepšení lze například výmahat plnění smlouvy. Tyto programy jsou dostupné všem a každý si může ověřit jejich funkčnost. Fakt, že tyto kontrakty jsou uloženy v blockchainu nám garantuje, že po zapsání se už nemohou měnit. Výhodou těchto typů konktraktu je skutečnost, že snižují náklady na ověřování plnění daného kontraktu a jeho vymahání a dále také slouží jako prevence vůči podvodu. Dá se říci, že chytrý kontrakt slouží jako automatizovaný právník a soud.

Blockchain 2.0 však nepřinesl pouze chytré kontrakty, ale také mikrotransakce, které by v normálních systémech byly velmi neefektivní a drahé. Mohou to být transakce v řádů haléřů či centů.

Dálé narážíme na pojem chytré vlastnictví, který můžeme chápat jako koncept, který určuje vlastnické práva určitých věcí. Do budoucna tato myšlenka počítá s tím, že informace o vlastnictví bytu, domu nebo čehokoliv jiného budé zapsáno touto formou do blockchainu.

Typickou implementací blockchain 2.0 je Ethereum[6].

3.2.3 Blockchain 3.0

Postupem času se mezi námi našli lidé, kteří si uvědomovali hned několik souvislostí. Jestliže nám blockchain 2.0 umožňuje sdílet kód a každý si ho může spustit, tak proč ho nevyužít na tvorbu aplikací. A právě o této myšlence je třetí generace blockchainu, tvorba decentralizovaných a škálovatelných systémů. Tyto aplikace jsou známe pod zkratkou Dapps, tedy decentralizované aplikace. Dapps mají svůj především backendový kód uložený a prováděný v blockchainu, nicméně data a komunikace jsou rovněž ukládány, respektivě prováděny v blockchainu. Uživatelé blockchainu, kteří poskytují svůj výpočetní výkon nebo paměťový prostor pro tyto aplikace, jsou za tyto úkony odměňováni. Tyto aplikace musí mít plně otevřený kód, ale data musí být šifrována. Výhodou této architektury je vysoká odolnost proti výpadkům v síti, neboť backend a data jsou uloženy v blockchainu, tudíž nehrozí, že by někdo napadl jeden uzel a aplikace se stala nepoužitelnou. Frontend aplikace může být napsán v libovolném jazyce, který bude schopný volat backend v blockchainu. Blockchain třetí generace bude významným stavebním prvkem Webu 3.0. Nyní již existují první projekty, které vytváří pomocí blockchain 3.0 superpočítač, neboť počet počítačů v blockchainové síti je ohromný a jakmile se výkony spojí dohromady, dokaží konkurovat komerčním superpočítačům.

Nejznamější implementace blockchainu 3.0 je Cardano[15]. O této implementaci se rozepíši později níže.

3.2.4 Blockchain 4.0

Čtvrtá generace blockchainu není stále přesně definována, ale bude směřovat k maximálnímu využití v Průmyslu 4.0. Tedy především automatizace, plánování, škálovatelnost, bezpečnost a snadná kontrola. Mimojiné přinese také snížení nákladů a zvýšení efektivity.

3.3 Kryptografie

Kryptografie je nepochybně jedním ze základním stavebních prvků blockchainu. Bez kryptografie by nebylo možné garantovat bezpečnost celého systému. Blockchain využívá nejen šifrování, ale také kryptografické funkce pro tvorbu kontrolního součtu, jinými slovy otisku. Kvůli této skutečnosti je důležité, abych v této podkapitole uvedl základní pojmy a funkčnosti kryptografie, která se používá u blockchainu.

3.3.1 Šifrování

Šifrování je takový proces, kdy se nezabezpečená data a informace převádí na data šifrovaná, které posléze nejdou přečíst bez dešifrování. Nezašifrováným datům se v kryptografii říká otevřený text a zašifrovaným datům šifrovaný text. K šifrování a dešifrování je potřeba dodržet určitý postup nebo algoritmus a především mít správný klíč nebo klíče. Šifrovat a dešifrovat

data lze pomocí jednoho stejného klíče pro šifrování i dešifrování nebo pomocí dvojice klíčů, kde první slouží pro šifrování a druhý pro dešifrování.

- Symetrické šifrování

  Symetrické šifrování používá k šifrování i dešifrování jeden klíč. Tento způsob šifrování má nízkou výpočetní náročnost, a proto je velice rychlý. Toto šifrování má však jeden podstatný problém, je zde nutností předat klíč druhé straně. Právě sdílení tohoto klíče je velký problém a zároveň zranitelnost tohoto způsobu šifrování. Pro bezpečné přenesení klíče se začala používat kombinace symetrického a asymetrického šifrování.

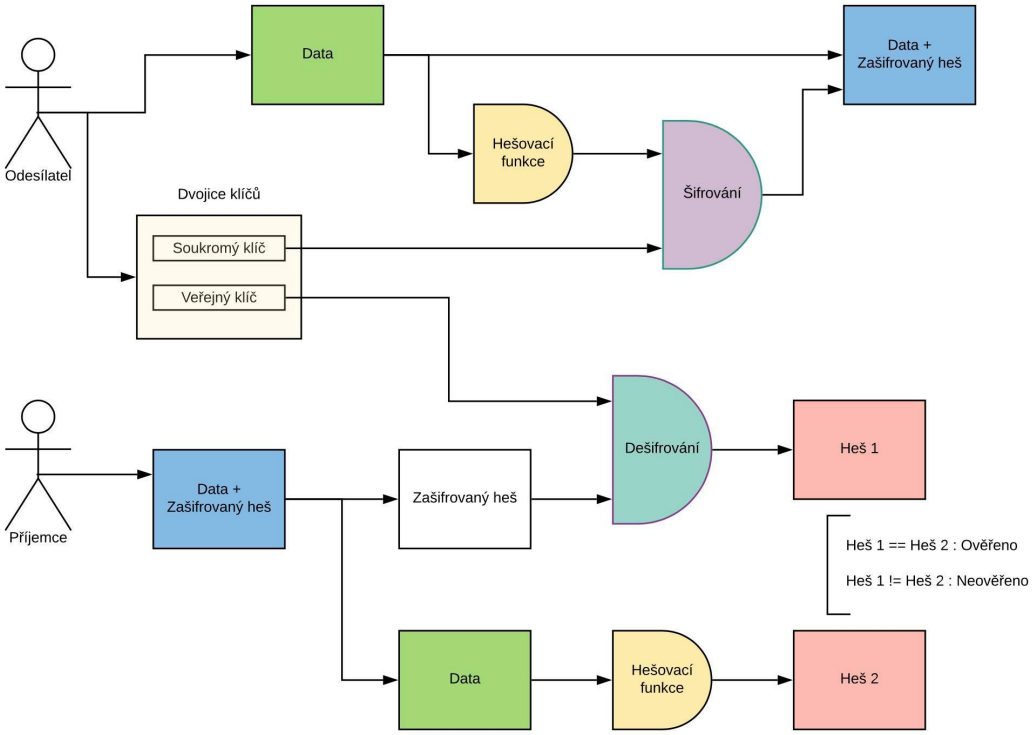
- Asymetrické šifrování

  Asymetrické šifrování používá 2 klíče. Tyto klíče se označují jako veřejný a privátní klíč. Jeden z těchto klíčů se použije pro zašifrování zprávy a druhý klíč následně pro dešifrování zprávy. Označení klíčů vychází z toho, jak je s nimi naloženo. Privatní klíč je pouze pro uživatele, který ho vytvoří a nikomu ho nesdílí, ale veřejný klíč může naopak sdílet všem uživatelům. U kryptoměn slouží veřejný klíč jako adresa a privátní jako podpis. Asymetrické šifrování lze rozdělit do dvou základních přístupů:

  – Veřejný klíč šifruje, privátní dešifruje - Tento přístup spočívá v tom, že veřejný klíč šifruje a privátní klíč dešifruje. V tomto případě nikdo nedokáže zjistit privátní klíč pro dešifrování a data jsou tedy tajná. Tento způsob se používá pro šifrování komunikace, kdy první strana poskytuje veřejný klíč a privátní klíč má pouze strana druhá. Díky tomu, že privátní klíč sloužící pro dešifrování má pouze druhá strana, nikdo nemůže danou zprávu odposlechnout. Jediný problém může nastat tehdy, kdy někdo zachytí prvotní zprávu, ve které vám druhá strana zasílá veřejný klíč pro šifrování. V tomto případě se může vydávat za první stranu.
  – Privátní klíč šifruje, veřejný dešifruje - Tento způsob většinou netají odesílané informace, ale pouze zaručuje jejich pravost. Využívá se toho i u kryptoměn, kde se takovým způsobem šifrují transakce, respektivě každý uživatel použije svůj privátní klíč na zašifrování kontrolního součtu transakce a každý si prostřednictvím veřejného klíče může ověřit, jestli danou transakci zašifroval on nebo ne.

3.3.2 Digitální podpis

Digitální podpis je způsob, jakým lze ověřit v elektronické komunikaci, zda danou zprávu odeslal správný uživatel. Je založeno na asymetrickém šifrování, jinými slovy že privátní klíč šifruje a veřejný dešifruje. Smyslem podpisu není data zatajit, tudíž zpráva se nešifruje celá, ale pouze časové razítko a kontrolní součet a tato šifra se přidá ke zprávě. Každý posléze prostřednictvím veřejného klíče odesílatele dokáže tuto šifru dešifrovat a zkontrolovat jestli po dešifrování odpovídá časové razítko a kontrolní součet s danou zprávou. Schéma digitálního podpisu je zobrazeno na obrázku 7.



Obrázek 7: Digitální podpis

3.3.3 Hešovací funkce

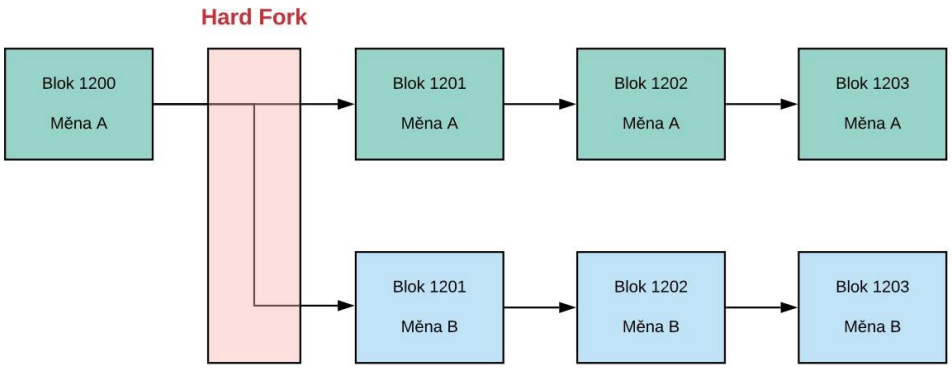
Hešovací funkce slouží k vytváření kontrolních součtů ze vstupních dat. Je to jednosměrný proces, kdy ze vstupních dat získáme heš (kontrolní součet), ale z tohoto heše již nelze získat zpět vstupní data. Výpočet heše by měl být rychlý, ale především jednoznačný, respektivě pro stejná vstupní data musí být vždy stejný heš. Zároveň by nemělo docházet ke kolizím, což znamená, že 2 různé vstupy vedou ke stejnému heši. Výstup z hešovací funkce má většinou pevně danou délku pro libovolně velký vstup.

3.4 Části blockchainu

V následující podkapitole popíši jednotlivé části blockchainu, k čemu slouží a co v nich najdeme. Zaměřím se primárně na blockchain 1.0 pro digitální měnu.

3.4.1 Protokol

Protokolem rozumíme hlavní část, která definuje, jak se celý blockchain bude chovat. Protokol definuje, jaké algoritmy budou použity, jaká bude velikost bloků, jaká bude složitost těžby a mnoho dalšího. Během jeho používání se dá také upravovat a to i zásadně, nicméně pak mohou vznikat tzv. forky. Fork můžeme chápat jako aktualizaci. Rozlišujeme dva druhy forků:



Obrázek 8: Ukázka Hardforku

- Soft fork - Je změna v protokolu, která je i zpětně kompatibilní. Většinou se jedná o malé změny). Uzly se starou verzí protokolu dokáží dále fungovat, ale mohou být částečně limitovány.

- Hard fork - Zde se jedná o větší změnu a je zpětně nekompatibilní. To znamená, že pokud uzel neaktualizuje svůj protokol, nebude schopnen dále nový blockchain používat. Jako hard fork označujeme i vytvoření zcela nezávislého nového blockchainu, přičemž starý může dále pokračovat. Příklad hard forku je na obrázku 8.

3.4.2 Uzel

Uzlem nazýváme zařízení, na kterém běží daná instance blockchainu. Více uzlů dohromady vytváří blockchainovou síť. Každý jeden uzel je důležitou součástí blockchainu.Existuje více typů uzlů, to znamená, že ne všechny uzly plní stejnou roli. Uzly rozlišujeme na:

- Plný uzel (Full node) - Plný uzel je jeden z nejdůležitějších uzlů, neboť obsahuje celou kopii blockchainu. Uzel udržuje blockchain stále aktuální, aby mohl validovat transakce, které přicházejí a dále je mohl přeposílat. Dále může poskytnou kopii blockchainu novým uzlům. Je tedy zřejmé, že je to hlavní základní stavební prvek celé blockchainové sítě. Díky tomu, že obsahuje celý blockchain a zároveň validuje transakce je tento uzel náročný na HW. Mimojiné ho lze použít i jako peněženka. Za zmínku stojí také tzv. Super uzel (Super node), což je plný uzel, který je nepřetržitě zaplý a má na sebe navázáný velký počet uzlů.

- Lehký uzel (Lightweight node) - Tento uzel neobsahuje celou kopii blockchainu, ale pouze části, většinou záhlaví bloků. Tyto uzly vytváří, přijímají a přeposílají transakce. Takové uzly se připojují alespoň k jednomu plném uzlu. Provozovat tento uzel nevyžaduje takové složité výpočetní prostředy jako plný uzel. V tomto případě není uzel schopen úplně

kontrolovat transakce, neboť neobsahuje již výše zmíněný celý lockchain, ale pouze jeho záhlav. Avšak i přesto dokáže blockchainové síti pomoci tím, že umí ověřit zjednodušené kontroly plateb (SPV), zdali je transakce v bloku a nebo není. Toto se zprostředkovává prostřednictvím sofistikované techniky známe jako Merkleovy stromy. Tato technika spočívá zjednodušeně v tom, že žádné dva bloky nemají stejnou větvičku Merkle a jsou zcela jedinečné. Tímto dokáže odfiltrovat falešné transakce a zamezit jejímu šíření v síti, tedy odlehčit síti.

- Těžební uzel (Mining node) - Těžební uzel se stará o potvrzování nových bloků a jeho přidávání do blockchainu. Je to uzel, který potřebuje velmi výkonný HW, aby dokázal rychle potvrzovat nové bloky, neboť jak si později vysvětlíme, potvrzování nového bloku je velmi výpočetně náročné. Nyní se již nepoužívají pro provoz těchto uzlů běžné počítače, ale spíše specializované zařízení (ASIC) a nebo počítač s několika grafickými kartami. Tyto uzly jsou pro funkci ztěžejní, a proto aby měli lidé motivaci tyto uzly provozovat, je každý nově potvrzený blok tímto uzlem odměněn.

- Směrovací uzel (Routing node) - Směřovací uzel je schopnž předávat jiným uzlům informace o síti, např. adresu jeho souseda. Vytváří celou síťovou část blockchainu. Většinou všechny uzly obsahují funkcionalitu směrovacího uzlu.

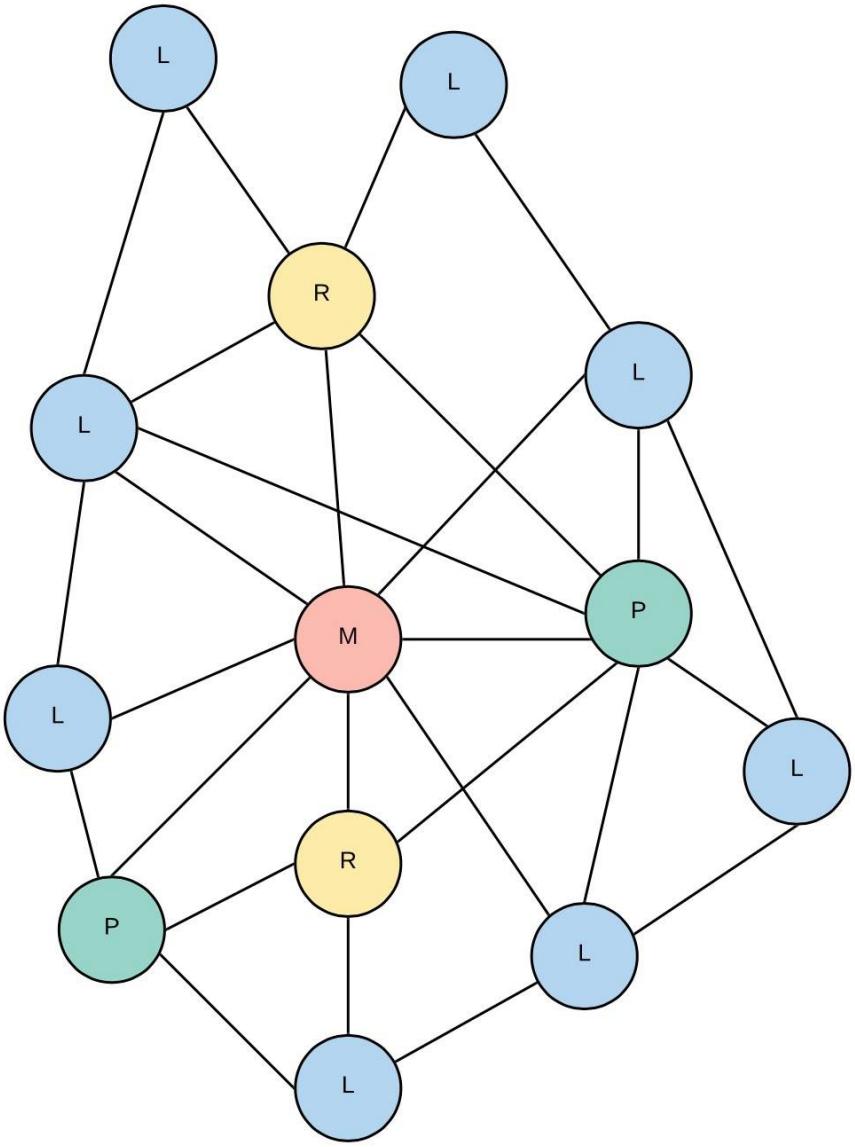
3.4.3 Blockchainová síť

Blockchainová síť je decentralizovaná P2P počítačová síť, ve které neexistuje žádný centrální prvek a skládá se z uzlů. K připojení do sítě potřebujeme znát adresu alespoň jednoho uzlu, který v síti je. Většina uzlů má ve zdrojovém kódu natvrdo zapsáno několik IP adres uzlů nebo IP adresy tzv. DNS seeds, které průběžně udržují seznam aktivních uzlů v síti. Příklad toho jak může blockchainová sít, je vidět na obrázku 9.

3.4.4 Peněženky

Definovat pěněženku v blockchainu není úplně jednoduché a může být zavádějící. Každý si představí, že ve své peněžence má něco uloženo a pokud se bavíme o např. digitální měně, tak očekáváme, že v dané peněžence se bude daná měna uchovávat. Ale tak to není a dokonce i přesto, že se jedná o digitální měnu, můžeme mít doslova peněženku vytištěnou na papíře. Díky tomu, že celý blockchain je založen na kryptografii, tak hlavní práci peněženky je pracovat právě s kryptografickými funkcemi. Peněženky využivájí asymetrickou kryptografii, tedy kryptografii založenou na dvou klíčích, jak již bylo řečeno, jedná se o veřejný a soukromý(privátní) klíč.

Hlavní funkcí peněženky je spravovat kryptografické klíče a to i na papíře. Veřejné klíče zároveň slouží ke generování adresy peněženky. Z toho plyne, že peněženku můžeme mít uloženou kdekoliv a pouze pokud chceme odesílat transakci, tak je potřeba údaje z peněženky použít. Zároveň můžeme platby přijímat, protože informace o tom, že jsme obdrželi na naši adresu



Obrázek 9: Blockchainová síť

platbu je uložena v blockchainu. Peneženkou je libovolný uzel i speciální uzel, který slouží pouze k odesílání transakce.

3.4.5 Transakce

Transakce je základní stevební prvek bloků, nicméně dá se říci, že doslova celého blockchainu. Transakce představuje něco jako jeden záznam v klasické databázi. Skládá se minimálně z:

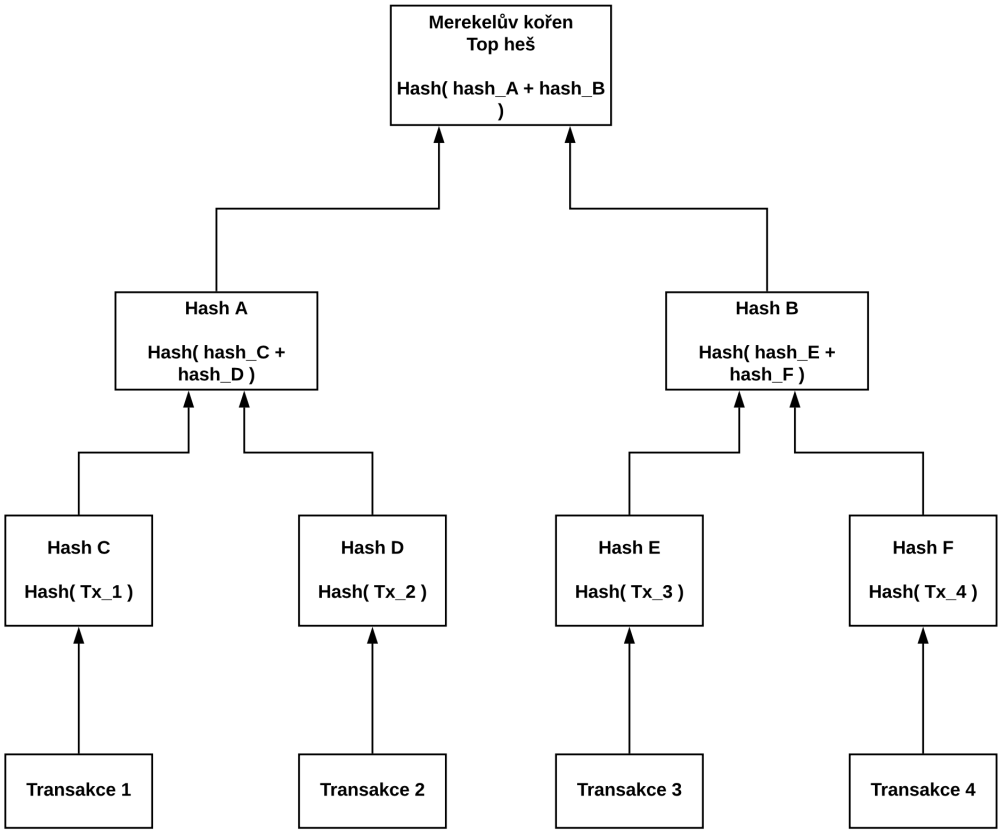
- Časové razítko
- Vstupy
- Výstupy
- Částka
- Poplatek
- Veřejný klíč odesílatele
- Digitální podpis odesílatele
- Kontrolní součet

Pokud by se jednalo o nějakou sofistikovanější verzi, může toho obsahovat více.

3.4.6 Bloky

Tak jak je popsáno již na začátku, že blockchain je řetězec bloků, tak nyní se dostáváme k vysvětlení, co konkrétně blok znamená. Blok simuluje jakýsi box, do kterého se vkládají transakce a vždy po nějakém čase nebo počtu, v závislosti na tom jaké je nastavení blockchainového protokolu, se tento box zavře. Blok se skládá z transakcí a hlavičky, která obsahuje:

- Verze
- Časové razítko
- Aktuální složitost
- Nonce
- Kontrolní součet předchozího bloku
- Merkelův kořen



Obrázek 10: Merkle Tree

Blok potvrdí (vytěží) těžební uzel (těžař), který najde odpovídající nonci. Nonce je vygenerované číslo, které ovlivňuje výsledek kontrolního součtu tak, aby odpovídal aktuální složitosti. Například aktuální složitost je nastavená tak, aby kontrolní součet začínal třemi nulami. Poté ještě mezi transakce přidá tzv. Coinbase transakci, což je odměna těžaři za nalezení správné nonce, respektivě vytěžení tohoto bloku. Výše odměny závisí na nastavení blockchainového protokolu a součtu poplatků transakcí daného bloku.

3.4.7 Merkle Tree

Jinými slovy stromová struktura, která využívá hešovací funkce na zajištění integrity dat v této struktuře. Všechny listy obsahují heš, v případě použití v blockchainu je to heš transakce. Merkle Tree se vytvoří tak, že se dané heše spojují a změna jakéhokoliv heše ovlivní výsledný heš, který je v nejvyšším uzlu, kterému se říka Merkelův kořen. Na obrázku 10 je ukázano jak takový strom vypadá.

3.5 Jak blockchain funguje?

Opět se zaměřím především na blockchain 1.0, na kterém se funkčnost dobře vysvětluje. Vyšší verze se liší poze v tom, že mají další funkcionalitu jak jsem popsal v kapitole 3.2. Nyní přejdu k vysvětlení funkcionality od základu. Popíši jaké procesy se během fungovaní dějí, a to od vzniku prvního bloku až po velkou síť s tisícemi uzly.

3.5.1 Připojení se k blockchainové síti

Jako první věc, za předpokladu, že již máme naisnatalovaný SW daného uzlu, musí proběhnout připojení do sítě. Tento úkon není vždy úplně jednoduché, neboť jak jsem již výše zmínil, blockchainová síť je decentralizovaná P2P síť, proto zde není žáden centrální prvek, kde můžeme ihned uzel připojit. Většina SW má v sobě uloženo několik fixních IP adres uzlů, na které se pokusí připojit po prvním spuštění. Pokud se podaří k některým připojit, může uzel požádat ať mu tento uzel pošle určitý počet jeho sousedů. Pokud by se připojení navázat nepodařilo, existují ještě DNS seeds IP adresy nebo adresy domén, které by měly běžet nepřetržitě. Tyto DNS seeds udržují neustále seznam některých aktivních uzlů. Každá implementace SW daného uzlu většinou používá jiný počet, jiné fixní uzly a DNS seeds.

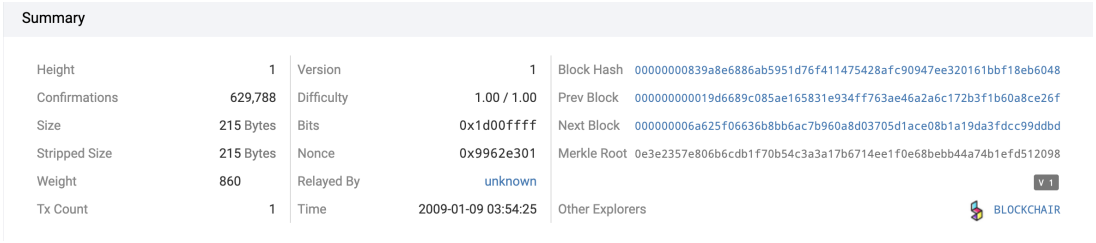
Následně si každý uzel uloží určitý počet sousedů a ten se snaží udržovat s pomocí stejných postupů. I když uzel odpojíme od sítě, měl by si uložit všechny uzly, ke kterým byl připojený, protože při dalším připojení k síti by měl prvotně zkusit obnovit spojení s nimi a v případě neúspěchu by měl použít postup, který se používá při prvním připojení. Tento postup má několik důvodů:

- Snižení zátěže těchto fixních uzlů a DNS seeds. Pokud by při každém připojení uzlů do sítě byla snaha připojit se k těmto uzlům, vzikala by velká zátěž na uzly.
- Pokud by se všichni připojovali vždy tímto způsobem, hrozil by vznik centrálních uzlů, které by mohly být poté zneužity, např. ignorování některých transakcí.

3.5.2 Genesis blok

Genesis blok je první blok daného blockchainu. Může být označován i jako Block zero, ale nejčastěji se setkáváme s názvem Genesis blok. Jako zajímavost je vhodné zmínit, že v Genesis bloku Bitcoinu je zapsáno "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks". Tento genesis blok je vidět na obrázku 11.

Tento blok představuje jakýsi vzor pro všechny další bloky. Je to jediný blok, který nemá z podstaty věci kontrolní součet předchozího bloku. Právě zmiňovaný blok je v kódu naprogramován natvrdo. Zajímavostí je fakt, že první odměnu za nalezení Genesis bloku nelze utratit. Vytváří se zde otázka, kdo nebo jak může provést platbu. To je ovšem celkem jednoduché. Jednoduše se vytěží druhý blok, který neobsahuje žádnou transakci a odměnu za vytěžení tohoto



Obrázek 11: Genesis blok Bitcoinu

bloku už lze přeposílat. A takto přesně vypadají první bloky blockchainu. Samozřejmě by šlo naprogramovat to, aby se dala přeposlat odměna z Genesis bloku, ale vývojáři drží tradici, kterou založil Satoshi Nakamoto.

3.5.3 Peněženky

K tomu, aby se dala odeslat, ale nejdřív vůbec přijmout nějaká digitální měna, je potřeba mít vygenerovanou adresu. Adresy se tvoří na základě klíčů a ty se generují klasicky pomocí různých algoritmů asymetrické kryptografie. U kryptoměn je oblíbené používat kryptografii nad eliptickými křivkami. Následně se z veřejného klíče spočítá kontrolní součet a ten může být použit jako adresa. Je samozřejmostí, že adresa se může generovat i sofistikovaněji, např. Bitcoin používá algoritmus ECDSA Secp256k1 pro generování klíčů a adresa vzniká takto:

1. Vygeneruje se privátní klíč na základě seznamu slov (seed phrase) nebo úplně náhodně.
2. Na základě privátního klíče se vygeneruje veřejný komprimovaný klíč o velikost 33 bajtů, skládající se z přípony 0x02 nebo 0x03 a 256 bitového čísla.
3. Z veřejného klíče se spočítá kontrolní součet algoritmem SHA256.
4. Z kontrolního součtu se vytvoří další kontrolní součet, ale tentokrát algoritmem RIPEMD-160.
5. Na začátek kontrolního součtu se přidá bajt (0x00), což je verze adresy. V případě testovací Bitcoinové sítě se používá bajt (0x6F).
6. Následně se opět provádí kontrolní součet pomocí algoritmu SHA256.
7. Poté se uloží první 4 bajty tohoto kontrolního součtu.
8. 4 bajty z předchozího kroku vložíme nakonec kontrolního součtu z 4. kroku.
9. Nakonec převedeme výsledek z 8. kroku pomocí Base58Check a dostaneme Bitcoinovou adresu.

3.5.4 Vytváření a posílání transakcí

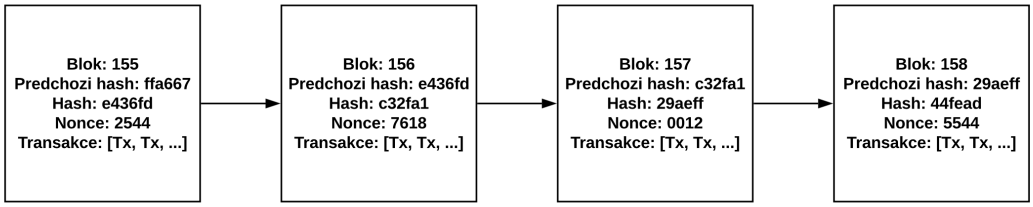
Každý uzel může transakce přijímat a přeposílat. Pokud je součástí uzlu i peněženka, může transakce vytvářet, avšak pod podmínkou, že má k dispozici nějaký zůstatek. Transakce tvoří základní stavební kámen celého blockchainu a jsou nesmírně důležité pro celé fungování blockchainu. Vytvoření transakce tedy požaduje, aby daný uzel obsahoval peněženku, měl nenulový zůstatek a znal adresu, na kterou chce transakci odeslat. Pokusím se to vysvětlit na vzorové transakci, kdy adresa A chce poslat 10 jednotek digitální měny na adresu B. Postup vytváření této transakce bude vypadat takto:

1. Jako vstup transakce se použije naše adresa, v tomto případě A, na které je dostatečný zůstatek k uskutečnění transakce.
2. Jako výstup transakce se použije adresa, na kterou chceme danou transakci uskutečnit. V tomto případě adresa B.
3. Zapíše se částka, kolik dané měny se má odeslat a také poplatek, který se většinou určuje podle aktuálního vytížení sítě a důležitosti transakce, tedy pokud je potřeba transakci provést co nejrychleji, je vhodne dát poplatek vyšší.
4. Pro následné ověřovaní se vloží veřejný klíč vstupní adresy. Tedy veřejný klíč adresy A.
5. Následně je potřeba vyplnit časové razítko a spočítat kontrolní součet této transakce.
6. Nyní se použije tajný privátní klíč k adrese (V tomto případě privátní klíč A) na vstupu a pomocí něho se podepíše tato transakce a to např. zašifrováním kontrolního součtu.
7. Nyní je transakce připravena k odeslání.

Transakce je vytvořena a může být odeslána do sítě. Veškeré transakce, i ty které se pouze přeposílají, postupují podle stejného principu. Jinak řečeno, každý uzel si uchovává určitý počet IP adres sousedních uzlů, na které potom broadcastuje transakce. Takže i tato vytvořená transakce se odešle všem uzlům, které si tento uzel ochovávají.

3.5.5 Validace transakce

Předtím, než se samotná transakce potvrdí a je zařazena do bloku, je validována. Validace je proces, kdy transakce, která dorazí do nějakého uzlu, který není těžař, je zkontrolována podle dostupných možností daného uzlu. Možnost ověření každého uzlu je ta, zda sedí kontrolní součet a digitální podpis. Plný uzel může transakci validovat i více do hloubky a to tak, že v blockchainu ověří, zdali odesílatel vlastní dostatek prostředků pro provedené transakce. V případě, že uzel narazí na neplatnou transakci, tak ji zahazuje a dále nepřeposílá. Tento proces šetří kapacitu sítě, zvyšuje bezpečnost a podporuje decentralizovanost blockchainu.



Obrázek 12: Propojení bloků

3.5.6 Těžba

Mining neboli těžba hraje klíčovou roli celého blockchainu. Tím, jak funguje, zamezuje podvodům, např. dvojí útrata, falšování transakci. Každá jedna transakce, která je provedena, musí projít potvrzením/vytěžením a to tak, že je zařazena do bloku, který je umístěn do blockchainu. Tyto bloky mohou vznikat buď v pravidelných intervalech nebo při určitém počtu transakcí a podobně. Schéma jak jsou bloky propojeny je vidět na obrázku 12. Tento obrázek také zachycuje podstatné informace, které se berou v potaz při těžbě.

Těžba je zjednodušeně řečeno hledání řešení matematické hádanky, kdy těžař kromě kontroly, zdali transakce, které chce umístit do nového bloku nejsou neplatné, musí najít odpovídající nonci. To, jakou nonci hledáme, ovlivňuje aktuální složitost pro vytváření nových bloků tak, že se vyžaduje, aby výsledný kontrolní součet bloků začínal sekvencí n nul. Pro představu zde uvedu vzorový případ těžby bloku:

1. Těžař neustálé dostává spousty nepotvrzených transakcí a ty si ukládá. Seznamu nepotvrzených transakcí se říká mempool.

2. Těžař začne vytvářet nový blok tak, že vybere z mempoolu transakce, dle jeho vlastních kriterií. Většinou vybírá ty s nejvyšším poplatkem.

3. Jakmile má vybrané transakce v bloku, začne vypočítávat kontrolní součet na základě hlavičky tohoto bloku. To ovlivňuje, zdali splňuje podmínky aktuální složitosti.

4. Nyní se generuje nonce tak dlouho, dokud nenarazí na kontrolní součet, který splňuje formát aktuální složitosti nebo dokud jiný těžař nevytěží blok dříve.

5. Pokud těžař nalezne správnou nonci jako první, okamžitě pošle tento blok do sítě a začne těžit další blok. V případě, že někdo jiný vytěžil blok dříve, musí začít znova a zkontrolovat svůj mempool, jestli již některé transakce nebyly potvrzeny v novém bloku.

Samozřejmě nic není dokonalé a může se stát, že 2 těžaři mohou nalézt nonci téměř ve stejném čase. V tomto případě se dočasně blockchain rozvětví a až další blok určí, který blok se bude považovat za vytěžený a to na základě hlavičky, ve které bude uvedeno, který blok je

předchozí. Proto nemůžeme transakci považovat za potvrzenou již po prvním vytěžení, neboť není jisté, že neexistují 2 bloky se stejnou výškou bloku.

Tento druh těžby a tedy potvrzování bloků je nazýván PoW(Proof of Work), neboli doklad o práci. Je to jeden z mnoha konsenzuálních algoritmů jak potvrzovat transakce a přidávat nové bloky.

3.5.7 Konsenzuální algoritmy

Dříve zmíněné potvrzování bloků a přidávání jich do blockchainu určuje jakýsi konsenzuální algoritmus. Nyní popíši nejznámější a nejpoužívanější konsenzuální algoritmy.

- Důkaz o práci (PoW - Proof of Work)

  Tento algoritmus se používá především u kryptoměn. Princip tohoto algoritmus je jednoduchý, neboť při vytváření a potvrzování nového bloku je potřeba splnit, podle aktuální složitosti, určitý tvar vygenerovaného kontrolního součtu. Kontrolní součet ovlivňujeme prostřednictvím nonce. Většinou si můžeme nonci představit jako jakési počítadlo, u kterého musí být splněna aktuální podmínka pro kontrolní součet, jinak se jeho hodnota stále zvyšuje jako obyčejné počítadlo.

  Nalezení takového kontrolního součtu je výpočetně náročné, ale následné ověření, zdali opravdu kontrolní součet odpovídá danému bloku a nonci, je velmi jednoduchý a rychlý.

- Důkaz validací (PoS - Proof of Stake)

  Mnohým vývojářům se nelíbila výpočetní a především elektrická náročnost při algoritmu PoW. Proto přišli s algoritmem PoS, který není tak výpočetně náročný. Tento algoritmus se začíná pomalu rozšiřovat mezi kryptoměny a snaží se být nástupcem PoW.

  Dá se říci, že těžba u tohoto algoritmu vlastně neexistuje, neboť se zde nevyskytují těžební uzly. To je způsobeno tím, že nový blok zařazují do blockchainu validátoři. Validátor aktuálního bloku si vybírá náhodně z množiny plných uzlů a vyšší pravděpodobnost mají uzly s vyšším zůstatkem dané kryptoměny. Vybraný uzel dostane za tuto validaci odměnu ve formě poplatků transakcí, které obsahuje daný blok. Pokud by se tento validátor pokusil o podvod a zařadil by nevalidní transakce, strhne se mu určitá část jeho zůstatku podle nastavení protokolu.

  Jakmile je nový blok zařazen do blockchainu, probíhá validace tohoto bloku ostatními uživately. Dá se říci, že je to hlasování uzlu v síti a sílá hlasu se určuje opět dle zůstatku jednotlivých uživatelů. Pokud by se některý uživatel snažil schválně hlasovat opačně, bude mu stržena částka z jeho účtu. Pokud hlasuje pro potvzení a blok je validní, získává odměnu.

- Potvrzení spálením (PoB - Proof of Burn)

Tento algoritmus opět řeší problematiku vysoké energetické a výpočetní zátěže především u algoritmu Proof of Work. Je velice neefektivní spotřebovávát obrovské množství energie a také nakupovat stále nový hardware k tomu, aby těžař našel nový blok. Proof of Burn chce, aby těžař musel stále investovat určité usílí, respektivě finance na to, aby mohl vytěžit nový blok.

Princip, jakým se snaží problematiku koncesa řešit, je takový, že těžař odešle přiměřenou částku na adresu, kterou nikdo nevlastní a dané prostředky již nepůjdou nikdy použít. Většinou se posílá na adresu v jiném formátu než jsou adresy běžné a hodnota transakce by měla být v přibližné výie poplatků transakcí v aktuálních blocích. Jakmile uplyne určitý čas nebo transakce získá určitý počet konfirmací, tak z důvodu bězpečnosti a nemožnosti vrácení transakce, může těžař vytvořit nový blok a odeslat ho do sítě a jako důkaz doloží onu transakci.

- Byzantská poruchová tolerance (BFT - Byzantine Fault Tolerance)

  Tento způsob se snaží vyřešit problém nepoctivého či nespolehlivého uzlu. Tyto uzly se snaží identifikovat pomocí validace nekonzistentní transakci a to tím, že každý uzel, který transakci přepošle zkontroluje jestli je tranksace konzistetní a přidá svůj hlas ANO / NE. Tím pádem, odesílatel a případně uzly, které nesprávně provedou validaci, jsou označené za nespolehlivé uzly.

  Tento algoritmus se často používá v kombinaci s PoW.

- Důkaz o kapacite (PoC - Proof of Capacity)

  Idea tohoto algoritmu je opět snížit energetické a hardwarové nároky na těžbu. A to takovým způsobem, že k výpočtu nepoužívá procesory, grafické karty či jiné speciální zařízení, ale k verifikaci používá paměť. Princip je takový, že těžař obětuje svou kapacitu paměti pro zapsání kontrolních součtů, které lze poté opakovaně používat. Konkrétně se tento algoritmus skládá ze dvou kroků:

  1. Vygenerování množství možných řešení. Každé řešení je sdruženo do noncí, přičemž každá jedna nonce obsahuje 8192 kontrolních součtů, které jsou uspořádány ve dvojicích (scoops) očíslovány od 0 do 4095.
  2. V druhém kroku uzly generují pro každou nonci čísla od 0 do 4095, tedy probíhá losovaní dané dvojice a pro tuto dvojici spočítá deadlines, což je čas od vytvoření posledního bloku po tento nový blok. Ten, kdo bude mít deadline nejkratší vyhrává a vytvoří nový blok.

- Důkaz o důležitosti (PoI - Proof of Importance)

  Tento algoritmus je podobný jako PoS. Každý uzel má importance score, které se vypočítává na základě zůstatku, počtu transakcí za posledních X dní, ale také podle importance

score adres, na které posílal transakce. Neposuzuje se pouze počet transakcí, ale také objem. Poté se vybere uzel, podle náhodného procesu, přičemž uzly s vyšším importance score mají vyšší pravděpodobnost výběru. Jakmile je daný uzel vybrán, má právo vytvořit nový blok.

- Důkaz o autoritě (PoA - Proof of Authority)

  Tento algoritmus se liší od ostatních tím, že požaduje po daném uzlu, aby prokázal svou identitu. Pokud uživatel chce vytvářet nové bloky v blockchainu, které využívá tento konsenzuální algoritmus, musí zveřejnit identitu, trestní bezúhonnost a další požadavky, které daná implementace vyžaduje. Využívá se spíše u soukromých či komerčních řešení.

- Důkaz o aktivitě (PoA - Proof of Activity)

  Tento algoritmus je jakýsi hybrid mezi PoS a PoW. Těžba zde funguje v první fázi stejně jako v PoW, ale po nalezení správné nonce není automaticky blok vytvořen, ale je prvně poslán do sítě. Následně podobně jako PoS se vyberou náhodně uzly, které ještě dané bloky musí validovat a až poté je zapsán do blockchainu.

Konsenzuálních algoritmů existuje celá řada a další pořád vznikají. Každý se snaží řešit tento problém jiným způsobem a kvůli tlaku ekologů se hledájí energeticky nenáročné implementace, které by i tak byly bezpečné.

3.6 Slabiny a problémy blockchainu

Blockchain není dokonalá technologie a existuje zde řada problémů či možností útoků. O to vážnější je situace u kryptoměn, kde uživatelé mají často velké finanční prostředky, neboť jejich odcizení by mohlo mít fatální následky na důvěru v blockchain.

3.6.1 Nová technologie

Jako první problém neboli slabinu můžeme shledat to, že blockchain je velmi mladá technologie a jako každá nová technologie přináší v sobě množství možných chyb a zranitelnost. Často se společnosti a komunita snaží implementovat nové nápady co nejrychleji, a právě tímto mohou bez dostatečné kontroly vytvářet chyby.

3.6.2 Efektivita

Velký problém blockchainu je jeho efektivita a to nejen při vytváření nových bloků, ale také při ukládání dat. Při vytváření nových bloků se často používá algoritmus PoW, který je velmi energeticky náročný a to je v kontradikci s nynější dobou, která směřuje ke snižování emisí a spotřeby elektrické energie.

Další problém může nastat tehdy, pokud chceme blockchain použít jako distribuované úložiště. Při představě, že bychom takto chtěli ukládat fotky nebo videa, by datová náročnost na

přenos v síti mezi uzly a také náročnost na kapacitu jednotlivých uzlů byla obrovská. Tento problém se často řeší částečnou centralizací, tedy v blockchainu se ukládají pouze kontrolní součty daných souborů, což nemusí být bezpečné, jelikož v případě výpadku centrálního úložiště se k datům nedostaneme.

Také je problém s rychlostí zapisování transakce, a to především v soukromém sektoru, kde je příliš pomalá, proto blockchain dává smysl především tam, kde je velké riziko útočníků a manipulací.

3.6.3 Soukromí

Soukromí můžeme považovat za výhodu, ale také nevýhodu blockchainu. Kámen úrazu je to tehdy, kdy běžný uživatel, který nejčastěji používá blockchain jako kryptoměnu a myslí si, že je anonymní. Často je to pouhá iluze, protože existuje mnoho způsobů jak daného uživatele identifikovat a to například IP adresa, informace o tom, kam transakce odesílá, zvěřejnění adresy pod přezdívkou na různých fórech, která může sloužit k následné identifikaci. Nicméně často lze také uživatele identifikovat hned při výměně peněz na kryptoměnu, tedy nejčastěji na burze, která vyžaduje identifikační údaje. Pro většinu uživatelů to nemusí být problém, protože často používají kryptoměny pouze jako investici či experimenty. V tomto případě je to spíše pseudoanonymní.

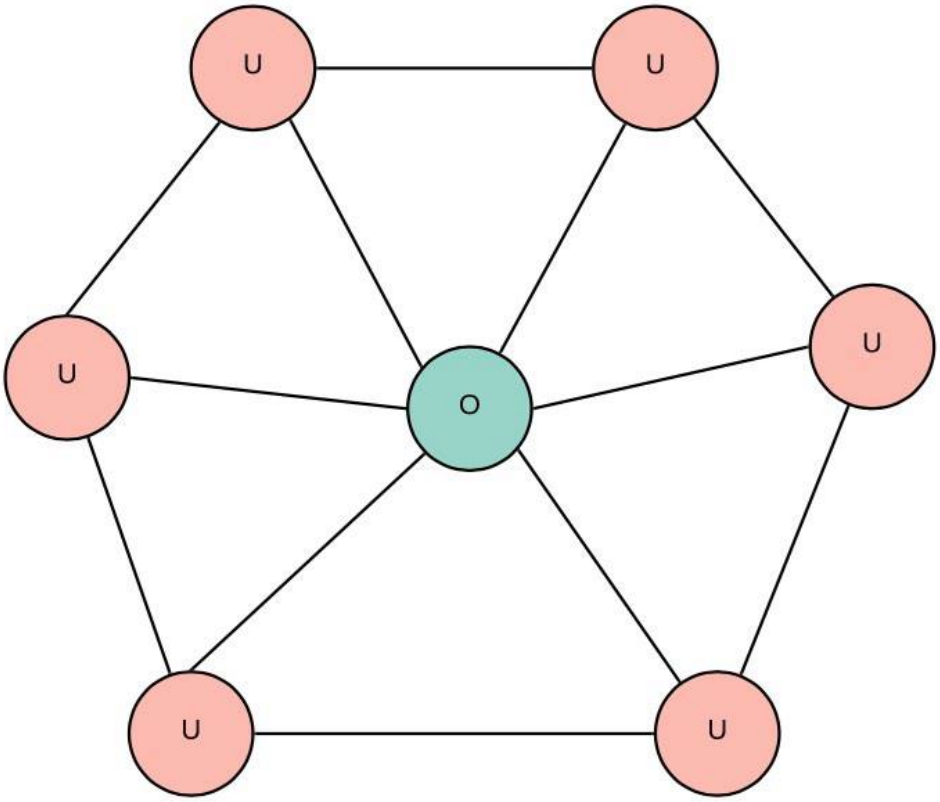
Naneštěstí je zde i druhá strana uživatelů, která má zkušenosti a využívá tuto anonymitu dokonale, především u kryptoměny Monero (XMR)[16]. Tito uživatelé používají blockchain, respektivě kryptoměny, k trestní činnosti a to například: nákup drog a zbraní, krácení daní či financování teroristických skupin. Jakmile se objevily kryptoměny, darknetový trh prudce vyrostl právě kvůli této anonymitě.

3.6.4 Bezpečnost a hacking

Bezpečnost blockchainu a hacking hraje u blockchainu velkou roli. Blockchain je z principu fungování zranitelný na určité druhy útoku. Nicméně kryptoměny, tedy implementace blockchainu, často zvyšují počet jiných hackerských útoku na běžné systémy, především ransomware, kdy útočník zašifruje data uživatelům a vyžaduje výpalné za odšifrování. Výpalné požaduje v podobě kryptoměny, která mu zaručuje anonymitu a jistotu, že ho nikdo na základě platby nevystopuje. Právě s rozšiřováním kryptoměn je tento typ útoků stále častější. Dále také objednání hackerského útoku je nyní snadnější a bezpečnější, neboť člověk, který si útok objedný, zaplatí v kryptoměně. Takže lze říct, že blockchain může i nepřímo ovlivňovat útoky na běžné systémy a zvyšovat jejich počet.

Existuje několik typů útoku na blockchain. Ty, které využívají zranitelnosti přímo v špatně napsaném kódu, kde chyba je především na straně vývojáře, ale také ty, které jsou přímo v technologii P2P sítě nebo samotné blockchainu, respektivě konsenzuálního algoritmu.

- Útok Eclipse



Obrázek 13: Útok Eclipse

Tento útok [17] zneužívá vlastností P2P sítě, respektivě šíření informací v blockchainové síti. Podstata útoku spočívá v tom, že útočník vytvoří několik útočných uzlů, které si následně oběť označí jako své sousedy. Pokud oběť bude mít všechny aktivní sousední uzly právě od útočníka, pak útočník dokáže veškerý provoz manipulovat. Pokud se tento útok podaří provést, tak hovoříme o období Man In The Middle, jelikož provoz mezi reálnou sítí a obětním uzlem směřuje vždy přes útočníka. Tímto způsobem můžeme oklamat oběť tím, že předložíme takový blockchain, ve kterém bude transakce, která reálně neproběhla. Znázornění tohoto útoku je na obrázku 13.

- Útok Sybil

  Útok Sybil [18] je z části podobný na útok Eclipse, ale je zde rozdíl. Útok Eclipse útočil na jeden vybraný uzel, ale útok Sybil útočí masivně na celou síť. Útočník přidá do sítě tisíce uzlů, kterými zaplavuje sousední uzly podvrženými informacemi. Cílem tohoto útok je vytvořit podmínky pro dvojí útratu či jiné manipulace v síti.

- Sobecký těžařský útok (Selfish mining attack)

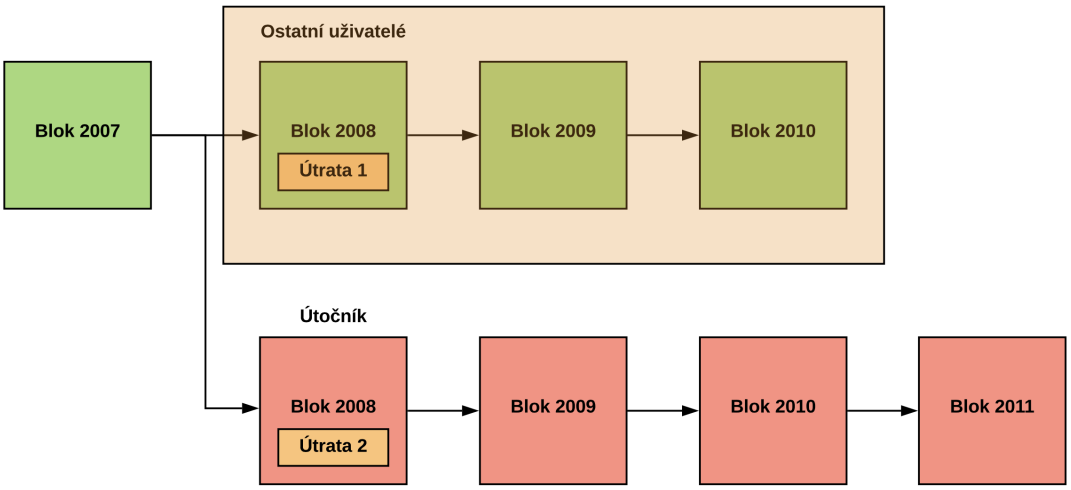
  Zde hovoříme o útoku, ve kterém těžař v případě vytěžení nového bloku nepošle tuto informaci do sítě a okamžitě pracuje na dalším bloku, což mu dává větší čas pro vytěžení následujícího bloku. Pokud se mu podaří nalézt i druhý blok, může pokračovat v těžbě a opět další blok neposlat do sítě, aby zvýšil pravděpodobnost vytěžení dalšího bloku, nebo pošle informaci do sítě. Díky tomu, že v blockchainu se nejdelší verze považuje za aktuální, budou ostatní verze považované za špatné a ostatní budou muset zahodit svou práci a začít těžit nový blok, který bude navazovat na verzi sobeckého těžaře. Tento útok není levný a snadně proveditelný, protože vyžaduje podstatnou část celkového výkonu sítě, ale u menších projektů je tento útok stále poměrně snadno proveditelný.

- Těžba Malwarem

  Tento útok nespočívá v útočení přímo na blockchain či P2P síť, ale využívá jiných zranitelností na uživatele internetu. Oběť nemusí být uzlem v blockchainové síti, může to být jakýkoliv uživatel internetu, u kterého se podaří útočníkovi získat přístup k výpočetnímu výkonu, který následně využívá pro těžbu kryptoměn. Tento útok je poměrně častý a některým útočníkům se podařilo získat výkon z více než milionů počítačů.

- 51% útok

  Podstata tohoto útoků [19] spočívá v tom, že útočník či většinou skupina útočníků, získá výkon větší než 51% celkového výkonu sítě. Tento útok lze provést především u menších projektů, kde celkový výkon není příliš vysoký. Pokud se tedy útočníkům podaří tuto podmínku splnit, dokáží manipulovat celým blockchainem, tedy zamítát transakce, provádět sobecký těžařský útok, ale i možnost dvojí útraty či jiné manipulace.



Obrázek 14: Ukázka 51% útoku

Útok může probíhat například tak, že útočníci zaplatí někomu markantní sumu, pošlou tuto transakci do sítě, ale mezitím vytváří vlastní verzi blockchainu bez této transakce a vlivem většího výkonu než 51% mohou mít útočníci po čase vytěženo 5 bloků bez jejich transakce. Zbytek těžařů bude mít pouze 4 bloky včetně bloku s jejich transakcí. Dále útočníci zvěřejní svou verzi blockchainu a díky většímu počtu bloků se jejich verze stane officiální verzí a jejich původní transakce bude zrušena. V případě, že transakce vedla například na burzu či Kryptomatu, mohla oběť tohoto útoku již vyplatit klasické peníze útočníkům či provést jiný úkon za tuto transakci, ale po zvěřejnění verze blockchainu od útočníků neobdrželi žádnou platbu. Schéma tohoto útoku je na obrázku 14.

- Útok přetížením (DDoS útok)

  Tento útok je velice známý, jelikož lze aplikovat na většinu dnešních systémů a technologií. Princip je jednoduchý. Cílem je pouze přetížit určité uzly či celou síť, což v případě sofistikovaného útoku může připravit podmínky pro další útok na blockchain.

3.7 Distribuované souborové systémy

Pokud je cílem použít blockchain i jako distribuované úložiště, je potřeba vyřešit problém, jaký souborový systém použít. Klasické souborové systémy nejsou schopné fungovat v P2P síti. Proto namísto klasických souborových systému bylo potřeba vymyslet nové distribuované souborové systémy, které budou schopné fungovat v podmínkach blockchainu.

U klasických systému se většinou data ukládají na lokální disk, případně na síťové úložiště, což většinou bývá vzdálený server, ke kterému přístupejeme skrz speciální protokol a nebo vytváříme síťový most a pracujeme s diskem jakoby byl lokální. K připojení k síťovým úložištím je potřeba znát IP adresu a cestu, kde se dané soubory nachází. Především klasické souborové

systémy mají centrální místo, kde se veškerá data ukládají, v lepším případě mají pár záložních kopií.

Distribuované úložiště toto všechno mění. Data jsou ukládána mezi více uzly, které nebízejí úložiště za poplatek. Tato data se dají vyhledat pomocí speciálního heše, což je unikátní identifikátor daného souboru či dat. Jestliže nějaký uzel chce určité data stáhnout, pošle do sítě požadavek s daným identifikátorem a nejbližší aktivní uzel, který tato data má, mu je zašle. Samotný přenos je poté rychlý a efektivní, protože síť se snaží vyhledat nejbližší uzly, ale na druhou stranu nějaký čas vezme právě vyhledání tohoto uzlu. Díky tomu, že data jsou replikována mezi všemi uzly, je tímto zajištěná vysoká spolehlivost a dostupnost.

3.7.1 Swarm

Swarm [20] je platforma pro decentralizovanou komunikaci a úložiště. Mezi hlavní její přednosti patří vysoká odolnost proti výpadkům a cenzuře. Uživatel, který chce data v síti uchovat, musí zároveň s daty zaplatit poplatek podle velikosti dat, které chce uchovat. Nejčasteji na této platformě jsou využívány k platbě chytré kontrakty prostřednictvím Ethereum.

Swarm umožňuje uchovávat zdrojový kód pro distribuované aplikace, ale také celý blockchain a uživatelská data. Tato platforma je v neustálém vývoji a vznikají stále nové projekty, které umožňují použít Swarm i jako hosting pro webové služby, ale také lze prostřednictvím této aplikace streamovat média.

Tento projekt vznikl kvůli platformy Ethereum. Nyní jsou tyto platformy vzájemně silně provázany. Uzly, které umožňují provoz této platformy nazýváme jednoduše Swarm uzly a každý tento uzel má svou speciální adresu, která je známá jako bzzkey.

Data nejsou ukládána jako celek. Než se nahrajou do sítě, tak se rozdělí na části, kterým se u Swarmu říka chunky, přičemž velikost 1 chunku je 4kB. Každý takový chunk je opět identifikován speciální adresou, které vzniká výpočtem hešovací funkce dat. Tyto chunky jsou poté distribuovány do sítě různými způsoby. Jeden ze způsobů, jak jsou tato data organizována, je Merkle tree, kdy jednotlivé uzly uchovávájí adresu daného chunku. Merkelův kořen v sobě nese heš, který jednoznačně identifikuje celý soubor nebo data.

3.7.2 Storj

Distribuované cloudové úložiště Storj [21] opět využívá provázání s Ethereum. Toto úložiště neslouží pouze pro potřeby blockchainu a distribuovaných aplikací, ale je nabízen i jako alternativa ke Cloudovým úložištím jako je Dropbox, Google Drive atd. Tento projekt nabízí jednoduchého klienta, který může sloužit jako vstup do sítě a umožní využívat volný prostor na disku a následně dostávat zaplaceno na danou adresu nebo lze použít jako vzdálený disk, kdy za poplatek lze ukládat data do distribuovaného cloudu.

Storj nabízí vysokou míru bezpečí, neboť data jsou podobně jako v případě Swarm rozděleny na části, zašifrovány a následně distribuovány mezi uzly. Díky tomuto faktu hostitelské uzly netuší, jaká data ukládají, protože nejsou jen rozdělena, ale právě i šifrována.

Storj má vlastní token / měnu prostřednictvím které vyplácí hostitelům odměny a uživatele v této měně platí. Mnozí uživatelé programu Filezilla ani neví, že tento program má v sobě implementovaného klienta Storj a pužít tuto platformu je velmi jednoduché, což činí projekt lehce rozšířitelný i mezi nové uživatele blockchainu.

3.7.3 IPFS

Je internetový protokol [22] pro P2P sítě k distribuci dat bez použití centrální autority. Tento protokol je napsán v jazyce Go, díky kterému je dostupný na všech platformách. Tento protokol je také napsán v javascriptu, proto ho lze využívat i v prohlížeči.

Cílem tohoto projektu je nahradit a vylepšit protokol HTTP, především v oblasti využití v distribuovaných sitítch a úložištích. Chce vyřešit stejné problémy jako blockchain samotný a to tedy bezpečí, transparentnost, odstranění centrálního prvku, nízkou efektivita a cenzuru.

Tento protokol neřeší přesnou adresu úložení dat, ale opět prostřednictvím speciální adresy identifikuje daná data. Protokol vyhledá konkrétní uzel, který požadovaná data má a to prostřednictvím distribuované hešovací tabulky a dalších technologií.

Pro uživatele, kteří nechtějí využívat protokol IPFS přímo, existuje alternativa formou IPFS brán, které fungují jako webová stránka na protokolu HTTP.

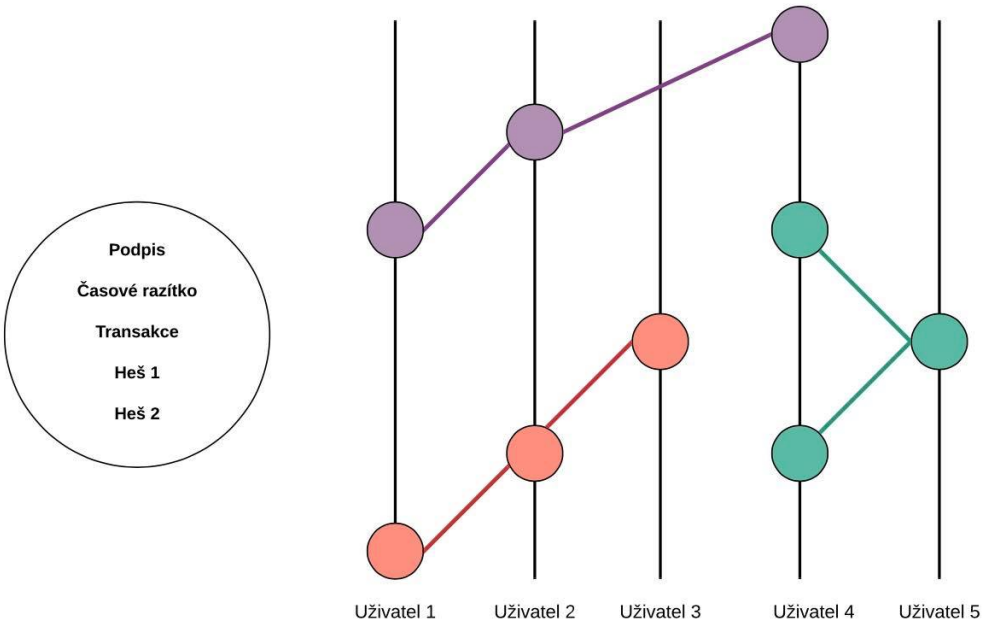
3.8 Alternativa k blockchainu

Blockchain není jedinná technologie, která se snaží přinést nové inovace do světa IT. Existuje spousta dalších řešení, které zvládají stejné věci jako blockchain a jeho aplikace. Každé řešení k různým problémům přistupuje jinak a já se pokusím některé z nich popsat.

3.8.1 Klasické systémy

Jako alternativu k dnešnímu blockchainu lze považovat i klasické metody pro práci s daty. Klasické databázové systémy, běžné souborové systémy či serverové aplikace jsou stále plnohodné technologie, které dokáží blockchain v mnoha případech porazit. U každého projektu je potřeba se zamyslet, která technologie bude nejlepší a nesnažit se za každou cenu upřednostnit jednu nad druhou. Pro soukromý sektor, který zpracovává tisíce transakcí za sekundu nebo zpracovává transakce, které není potřeba neustále zálohovat a ověřovat, je zbytečné nasazovat technologii blockchain.

Klasické technologie, pro velké množství tohoto druhu transakcí, jsou rychlejší a efektivnější. Dále existují data, která jsou vysoce citlivá, například vládní či armádní data, která by v případě použití blockchainu nebyla dostatečně v bezpečí. V případě zranitelnosti na úrovni ukládání dat a jeho šifrování, by znamenalo, že každý uzel, který by měl data u sebe, by je teoreticky mohl



Obrázek 15: Hashgraph

přečíst. Nabízí se tedy i řešení soukromých blockchainů, ale je opravdu třeba zvážit, jestli je jeho použití zapotřebí.

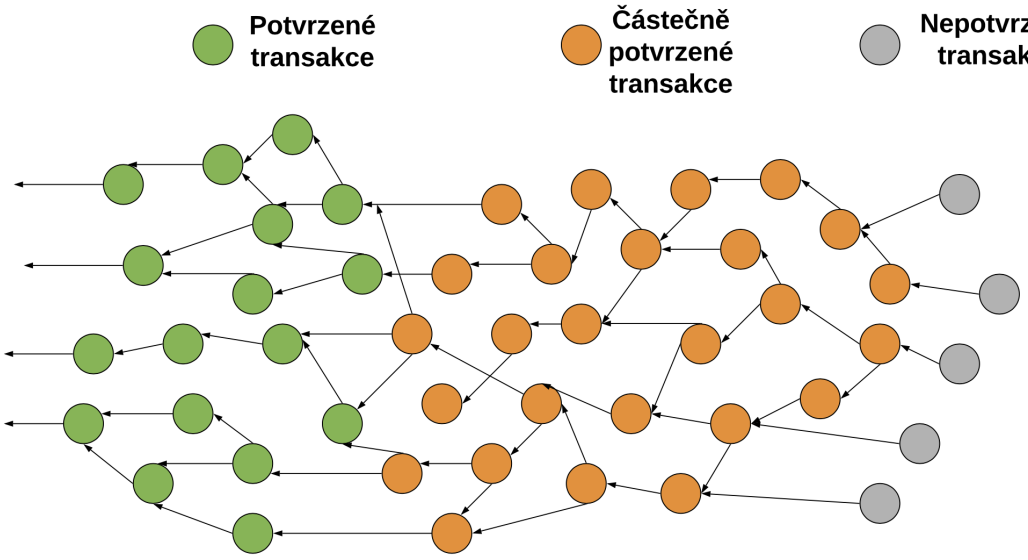
Klasické metody a technologie tedy jistě mají svá využití a příchod blockchainu pro ně neznamená, že by se automaticky staly zastaralé či nepoužitelné.

3.8.2 Hedera Hashgraph

Je to jedna z nejnovějších technologií [23], která se snažila navázat na úspěch blockchainu. Využívá částečně decentralizovanou síť, tudíž není plně decentralizovaným projektem a především nepoužíva blockchainovou strukturu pro ukládaní dat. Namísto blockchainu tedy využívá tzv. Hashgraph. Předností této technologie je vysoká rychlost zpracovávaní transakcí.

Architektura, kterou tento projekt používá, je známa jako DAG, což je orientovaný acyklický graf. Transakce se ukládají do událostí. Tyto události obsahují v sobě dva heše, transakce a časové razítko s časem provedení transakce.

V síti se neustále vybírají náhodně uzly, které následně přeposílají neprovedené transakce druhému uzlu, který je opět náhodně vybrán. Všechny obdržené transakce se zahrnou do nové události. Tento proces se děje v síti neustále a tímto dochází k potvrzování transakcí. Samotné odesílání transakcí je podobné jako v blockchainu, to znamená, že se posílají všem sousedním uzlům.



Obrázek 16: Tangle

Aby byla zachována integrita a bezpečnost, události musí mít 2 heše. První heš je referencí na poslední událost uzlu, ze kterého přišly dané transakce. Druhý heš obsahuje referenci na poslední událost, kterou daný uzel vytvořil. Následně danou událost digitálně podepíše uzel, který tuto událost vytvořil.

Následně je transakce potřeba validovat a to se provádí prostřednictvím virtuálního hlasování. Toto hlasování probíha v několika kolech, kdy se postupně hlasuje o daných událostech. Výhoda tohoto typu ověření je nízká výpočetní náročnost a vysoká propustnost. Obrázek 15 zachycuje tuto technologii.

3.8.3 Tangle

Tangle [24] je další technologie, která se snaží využít nejlepších vlastností blockchainu a přidat k nim něco víc. To hlavní, co přidává tato technologie, je rychlost zpracování transakcí a možnost provádět mikrotransakce, tedy transakce o nízké hodnotě, kdy často u blockchainu poplatky převyšují odeslanou částku.

Tuto technologii přinesl projekt IOTA. Vlastnosti, které tento projekt přinesl, umožnily nasazení této technologie do IoT. V této síti stejně jako v Hashgraphu neexistují bloky, ale ani jiné speciální shlukování transakcí. Každá jedna transakce se ukládá přímo do orientovaného acyklického grafu, respektivě každý uzel v grafu je jedna transakce a hrany jsou reference z jiné transakce, které jsou tímto novým propojením validovány. To znamená, že s rostoucím počtem uživatelů a transakcí, roste i rychlost zpracování transakce, což je opakem od blockchainu, protože tam je rychlost limitována vytvářením bloku.

Jednou z nejzásadnějších věcí zde je, že neexistují poplatky za transakci. Je k tomu pádný důvod, neboť poplatek je prováděn prostřednictvím služby, a to za validaci transakce, který se stane referencí při vytváření nové transakce.

Každá transakce v sobě nese množství informací. Podle jednotlivých implementací je nutné do každé transakce vložit referenci na X předchozích transakcí pro jejich zvalidování. Dále je nutností transakci digitálně podepsat a nalézt řešení určitého problému, jako například u Proof of Work, aby síť nebyla napadena v případě, že by nebylo žádným způsobem omezeno vytváření transakcí, což by mohlo vést k útokům prostřednictvím ohromného množství transakcí.

Každá transakce má svou kumulativní váhu důvěryhodnosti, že není zmanipulována. Tato váha se vypočítává na základě spotřebovaného výkonu pro nalezení řešení problému + váha následujících referencovaných transakcí.

Struktura tohoto grafu, která v sobě nese informace o všech transakcích, se neukládá v každém uzlu kompletně celá, ale pouze část grafu, která je pro daný uzel potřebná. Schéma této technologie je na obrázku 16.

4 Možnosti využití Blockchainu

Hlavní důvod proč je blockchain považován za revoluční jsou jeho možnosti využití. Na první pohled se to nezdá, ale jeho možnosti jsou obrovské. Celý finanční systém dnešní doby je velmi netransparetní a mnozí lidé vybízí k tomu, aby se přesunul na blockchain. Je otázka jak moc budou vlády a banky chtít, aby tyto informace byly veřejné. Ale jsou tady i jiné oblasti ve státní sféře, ve školství v IoT a mnoho dalších potencinálních možností.

Nedávno nám doba přinesla další zajimavé zjištění, kdy při zkoumání koronaviru bylo potřeba dát dohromady obrovský výkon. Soukromé, ale i státni organizace své superpočítače nabízejí za obrovské finance, ale lidé spojili síly a vytvořili distribuovaný superpočítač, který má výkon více než 10x větší než nejvýkonější superpočítač světa.

Všechny možnosti blockchainu jsou s vysokou pravděpodobnosti ještě neobjeveny a nové projekty budou stále přicházet. V této kapitole popíšu nejdiskutovanější oblasti použití.

4.1 Finanční sektor

Nelze začít ničím jiným než finančním sektorem. Díky popularitě kryptoměn lze vidět, že lidé o využití blockchainu v této oblasti mají zájem. V sektoru financí se nabízí přímo myšlenka využití blockchainu jako digitální měny. Dále možnosti využití vidím k určování vlastníka akcií či dluhopisů. Obrovský potenciál vidím také v použití chytrých kontraktů pro pujčování peněz.

Další možností je čím dál více oblíbené kolektivní financování s jistotou vráceni peněz při nevybrání cílového kapitálu. Tento sektor přímo vybízí k aplikaci blockchainu a uvědomují si to mnohé finanční instituce, které podporují množství blockchainových projektů.

4.2 Státní orgány

Státní sféra je další oblast, kde by lidé uvítali příchod blockchainu, aby se vše stalo přehlednější. Vlivem mnoha korupčních skandálů lidé přestávají věřit v to jak systém funguje a právě transparetní blockchain by to vyřešil. Ve státní sféře existuje mnoho procesů, které by měly být naprosto transparetní. Jako příklad mohou sloužit volby, dotace, ale také daňová přiznání či nové nařízení a zákony.

4.3 Školství

Školství je jednou z oblastí, kde by se blockchain mohl začít implementovat již brzy. Některé univerzity již začínají využívat jeho aplikaci na různé problémy. Právě na univerzitách jsou akademici, kteří nemají problém se rychle adaptovat na nové technologie a mohou takto otestovat možnosti aplikace i pro celé školství a další odvětví. Ve školství by se dal blockchain využít jako systém pro zaznamenavání hodnocení, docházky nebo také závěrečných prací.

4.4 Shrnutí

Možnosti blockchainu jsou tedy obrovské a dalo by se do nekonečna vymýšlet, kde by se dal uplatnit. Vybral jsem 3 sektory, který si dokáže většina lidí představit a nastínil možnosti jeho aplikace v daných oborech. Věřím, že již brzy se blockchainové technologie začnou nasazovat ve větším měřítku.

5 Vybrané Blockchainové projekty

V této kapitole popíši vybrané implementace blockchainu. Zaměřím se na klasické kryptoměny, ale také na tzv. Stable Coin, tedy stabilní měny a další zajímavé projekty.

5.1 Kryptoměny

Kryptoměny jsou stále nejvíce používanou implementací blockchainu. Není se čemu divit, protože právě kryptoměna Bitcoin byla první implementace blockchainu tak, jak ho známe dnes. Existují i jiné zajímavé kryptoměny a jejich počet postupně stále roste. V komunitě se označují kryptoměny jako digitální zlato a někteří lidé do nich investují velké částky. Investice do kryptoměn může být velmi výnosná, neboť v porovnání s klasickými finančními nástroji zde nacházíme větší cenové pohyby. Avšak právě tyto velké a prudké výkyvy cen mohou způsobit i velké ztráty. Obrázek 17 ukazuje 10 nejrozšířenějších a nejpoužívanějších kryptoměn.

5.1.1 Bitcoin

Bitcoin je první známý a masivně používáný projekt založený na blockchainu. Již výše zmíněný Satoshi Nakamoto v roce 2008 zveřejnil práci, tzv. White list, kde popsal fungování blockchainu a jeho využití pro elektronický platební systém bez centrální autority. Implementace Bitcoinu byla dokončena na konci roku 2008 a první blok, tedy blok Genesis, byl vytvořen 3.1.2009 s poznámkou "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks", což pro mnohé znamená rýpnutí si do klasického finančního systému.

Odpověď na otázku, proč zrovna prvním využitím blockchainu byla zrovna kryptoměna, není úplně jistá, ale může to mít souvislost s tím, že v roce 2007 začala velká finanční krize, která zasáhla celý svět. Tato krize byla vyvolaná právě centralními autoritami v klasickém finančním systému. Tato skutečnost mohla posloužit jako hlavní podnět pro vznik Bitcoinu. Vyřešil se tím problém zásahů centrální autority a to, že celý systém klasického finančního modelu je netransparetní.

Díky tomu, že vznikl v době krize a byl koncipiován opačně vůči klasickému finančnímu systému, se lidé začali o tento projekt zajímat a začali ho používat. To, díky čemu také získal Bitcoin zájem veřejnosti a investorů a poté všechny další kryptoměny, byl i opačný přístup ke vzniku nových mincí a jejich počtu. V klasickém finančním systému banky vytváří ohromné množství nových peněz, což způsobuje ztrátu jejich hodnoty a z historického hlediska se peněz vytváří stále více a už dávno nejsou ničím fyzickým kryté. To u mnoho lidí vyvolává otázku, jestli to je správné a zdali právě myšlenka Bitcoinu se toto snaží vyřešit.

Bitcoin vytváří nové mince podle přesně daných pravidel. Při vytěžení nového bloku dostane těžař odměnu. Takto vznikají nové mince. To, co by mělo zajistit, aby se tyto mince dostaly do oběhu, pramění z nároku na těžbu, tedy potřeby provozovat výkonné zařízení, které spotřebovává elektrickou energii a také potřeby často chladit. Aby si tyto podmínky na provoz mohl

Top 100 Cryptocurrencies by Market Capitalization

Cryptocurrencies ▾ | Exchanges ▾ | Watchlist | Filters | USD ▾ | Next 100 → | View All

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$161 625 077 498	$8 797,20	$59 030 037 521	18 372 325 BTC	-9,16%	
2	Ethereum	$21 154 780 511	$190,81	$23 516 931 417	110 869 449 ETH	-9,81%	
3	XRP	$8 807 895 746	$0,199667	$2 851 271 096	44 112 853 111 XRP *	-9,41%	
4	Tether	$6 361 632 402	$1,00	$72 922 938 080	6 361 032 509 USDT *	0,02%	
5	Bitcoin Cash	$4 348 124 890	$236,27	$4 892 616 648	18 403 213 BCH	-11,62%	
6	Bitcoin SV	$3 489 233 311	$189,61	$2 443 962 817	18 401 752 BSV	-10,59%	
7	Litecoin	$2 757 246 550	$42,62	$5 376 890 527	64 698 606 LTC	-10,83%	
8	Binance Coin	$2 398 946 545	$15,42	$428 451 962	155 536 713 BNB *	-9,47%	
9	EOS	$2 277 174 335	$2,47	$4 906 936 605	922 506 283 EOS *	-10,96%	
10	Tezos	$1 883 331 792	$2,65	$212 526 030	709 954 095 XTZ *	-6,80%	

Obrázek 17: TOP 10 kryptoměn k 10.5.2020

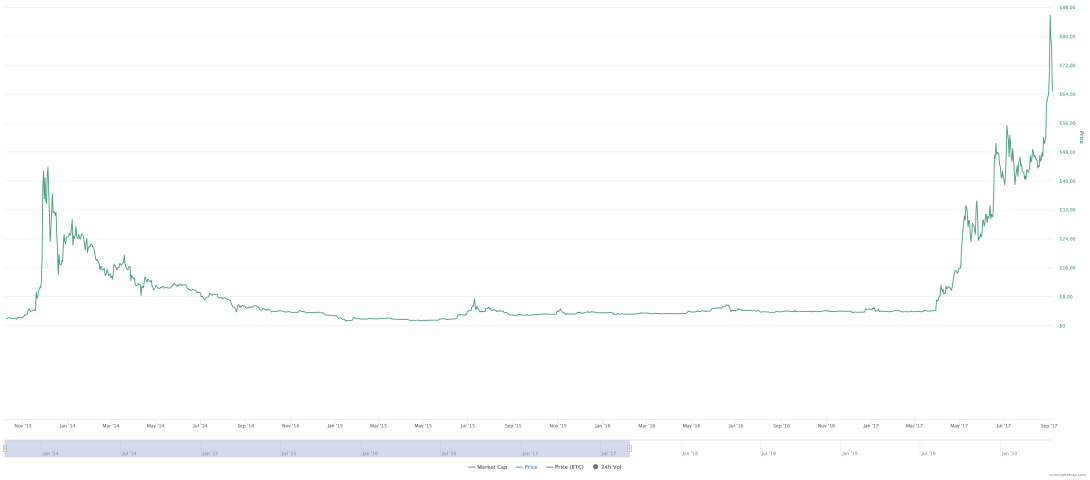
těžař zajistit, potřebuje alespoň část odměny převést či prodat někomu jinému, aby mohl platit účty za energii a kupovat nový hardware. Počet mincí za odměnu časem klesá, dochází k tzv. Halvingu neboli půlení odměny. Tento princip by měl zajistit růst hodnoty dané měny, protože nových mincí bude vznikat stále méně. Tento princip je přesně opačný vůči klasickému finančním systému. Bitcoin má však i další zvláštnost. Počet všech mincí, které budou existovat je 21 000 000, což znamená, že jakmile bude tato suma dosažena, těžaři již nebudou dostávat odměnu za vytěžení nového bloku, ale budou pouze závislí na poplatcích za transakce.

5.1.2 Litecoin

Tvůrce této kryptoměny je bývalý zaměstnance Google Charlie Lee. Cílem tohoto projektu bylo vylepšit Bitcoin, a tak se i stalo. Litecoin [25] je pouze upravený Bitcoin. Jedním z hlavních rozdílů a vylepšení je rychlost vytváření nového bloku, tím i tedy rychlost zpracování transakce a také četnost odměn pro těžaře. Litecoin ve srovnání s Bitcoinem je přibližně 4x rychlejší.

Průměrné poplatky za transakci jsou u Litecoinu nižší. Co se týče maximálního počtu mincí, vychází Litecoin z jednoduchého vzorce. Pokud má Bitcoin limit 21 000 000 a Litecoin je vytváří 4x rychleji, tak byl zvolen maximální počet 84 000 000.

Jednou z klíčových vlastností měl být algoritmus pro generování kontrolních součtů. Měl být odolný vůči speciální zařízením (ASIC) a zároveň jednodušší, aby se dal počítat na jakémkoliv počítači a nepodlehl stejnému trendu jako u Bitcoinu, kde se těžba rychle přesunula z klasických



Obrázek 18: Graf ceny LTC

počítačů na tzv. Rigy složené z grafických karet a následně na ASIC. Algoritmus Scrypt, který využíval Litecoin, nevydržel dlouho a brzy to bylo stejné jako u Bitcoinu. Tyto všechny události způsobily během roku 2014 pád hodnoty Litecoin o více jak 60% a samotný vývojář Charlie Lee oznámil, že již není potřeba další vývoj. Následně Litecoin zažil od roku 2014 až do začátku roku 2017 špatné období, kdy byl jeho vývoj pozastaven a hodnota byla nízká.

Začátkem roku 2017 vývojář Charlie Lee přiel s návrhem implementace SegWit a Lightning Network do Litecoinu a Bitcoinu. Tyto technologie umožnily zvýšit kapacitu sítě, zrychlit platby a také možnost mikroplateb. To však není vše, technologie SegWit vyřešila i některé zranitelnosti kryptoměn, například zranitelnost "Transaction Malleability". Ta spočívala v tom, že když uživatel A poslal transakci uživateli B, tak uživatel B mohl při přijetí nepotvrzené transakce pozměnit speciální skript, což změnilo ID transakce. Následně řekl uživateli A, že žádnou platbu nedostal a uživatel to zkontroloval na základě ID transakce a opravdu taková transakce neproběhla vlivem právě této chyby, že uživatel B mohl ID transakce pozměnit. Často se stávalo, že uživatel A zaplatil platbu 2x. Tato chyba vedla v roce ke krachu kryptoburzy Mt Gox. Od této doby se Litecoin začal opět silně prosazovat a patří mezi nejpoužívanější kryptoměny. Obrázek 18 ukazuje vývoj ceny Litecoinu v čase.

5.1.3 Ethereum

Koncept kryptoměny a platformy Ethereum [26] vznikl v roce 2013. O rok později Vitalik Buterin a Gavin Wood představili Yellow list a následně v 30.7.2015 spustili platformu officiálně. Důvodem, proč se zde hovoří o platformě a né jen o kryptoměně, je to, že Ethereum přišlo s několika novinkami, avšak mezi nejdůležitější řadíme příchod decentralizovaného turingovského kompletního virtuálního stroje Ethereum Virtual Machine, který umožňuje provádět chytré kontrakty. Hovoří se zde o kryptoměně další generace, protože implementuje blockchain 2.0.

Samotná měna se nazývá Ether a slouží primárně jako palivo pro celou Ethereum platformu. Ethereum vytváří bloky přibližně každých 12 sekund, díky čemuž je přeposílání transakcí v této síti opravdu rychlé. Díky chytrým kontraktům vzniká nespočet projektů skrz financování. Kvůli tomuto financování byl už v roce 2016 projekt Ethereum ohrožen a anonymní skupina ukradla 50 000 000 $ v Etherech. Kvůli tomuto hackerskému útoku bylo v komunitě velké pozdvižení, které vyústilo až k Hard forku a následně vznikly 2 další projekty. Ethereum a Ethereum Classic.

I přes všechny prvotní problémy a také časté financování podvodných projektů si Ethereum vydobylo pozici kryptoměnové dvojky hned po Bitcoinu.

5.1.4 Cardano

Projekt Cardano [27] lze považovat jako technologickou špičku ve využití blockchain technologiích. Impolementuje blockchain 3.0 a přináší blockchainu další možnosti. Cardano klade důraz na bezpečné převody skrz blockchain, ale také decentralizovanou směnnost jiných kryptoměn. Dále nabízí velice pokročilé chytré kontrakty a také prostředí pro vytváření decentralizovaných aplikací.

Cardano přišlo s vícevrstvým modelem, díky čemuž má mít větší fexibilitu a možnosti vývoje. První vrstva slouží primárně pro kontrolu a správu transakcí, tato vrstva se podobá Bitcoinu. Druhá vrstva se stará o chytré kontrakty a také dodržování synchronizace blockchainu. Tento projekt má samozřejmě svou měnu a její zkratka je ADA.

Vývoj začal v roce 2015 a součástí vývoje jsou mistři oboru z celého světa. Officálně bylo Cardano spuštěno v 29.9.2017. Tento projekt neběží jako většina projektů na konsenzuálním algoritmu PoW, ale využívá důkaz validací (PoS) a tudíž neplýtvá energií a výpočetními prostředky na hledání kontrolních součtů, a proto tento výkon může poskytovat uživatelům ve formě distribuovaných aplikací.

Avšak toto není vše. Cardano přichází s více vymoženostmi a má potenciál stát se jedním z nejvíce komplexních blockchainových projektů. Aktuálně na vývoji pracují špičkové univerzity z celého světa a společnosti či komunity nadšenců.

5.1.5 Srovnání

Z předchozích řádků můžeme dedukovat, že v dnešní době existuje řada projektů, které úspěšně implementují blockchain. Problémem pro mnohé může být to, že tápou v tom, jak se vůbec v těchto projektech vyznat, či jak je srovnat. Neexistuje žáden test, který by vyhodnotil, který projekt je nejlepší. Na další kámen úrazu narazíme tehdy, když si uvědomíme, že jednotlivé projekty implementují rozdílné verze blockchainu a to přináší možnosti, které nižší verze neumožňují. Pokusím se tyto projekty srovnat formou tabulky, kde porovnám vlastnosti, které jsou objektivně porovnatelné.

V tabulce 1 srovnávám verze blockchainu, algoritmy pro kontrolní součty, rychlost vytváření bloků, ale také cenu a tržní kapitalizace.

	Bitcoin	Litecoin	Ethereum	Cardano
Rok spuštění	2009	2011	2015	2017
Verze blockchainu	1.0	1.0	2.0	3.0
Konsenzuální algoritmus	PoW	PoW	PoW	PoS
Hodnota 1 jednotky měny	8 329 $	47 $	209 $	0.05 $
Celkový hodnota měny	152.8 mld. $	3.1 mld. $	23.2 mld. $	1.3 mld. $
Počet bloků	627 974	1 832 325	9 967 914	4 096 210
Rychlost vytěžení bloku	10 m	2.5 m	12 s.	20 s.
Počet transakcí	524 mil.	42.5 mil.	692 mil.	2 mil.
Výkon sítě	118 EH / s	176 TH / s	172 TH / s	-
Algoritmus pro kontrolní součty	sha256	scrypt Algorithm	keccak-256	BLAKE2b-256
Průměrný poplatek	0.66 $	0.015 $	0.14$	0.012 $
Chytré kontrakty	Ano, omezeně	Ano, omezeně	Ano	Ano
Decentralizované aplikace	Ne	Ne	Ano	Ano, ve vývoji

Tabulka 1: Srovnání vybraných blockchainových projektů k 28.4.2020

5.2 Stabilní měny založené na blockchainu

Stable coin neboli stabilní měna je speciální případ kryptoměny. Většinou to není přímo samotný blockchain, ale využívá se zde blockchcainu jiného, třeba od klasické kryptoměny. Stable coiny fungují často ve formě tokenů, které garantují, že kurz je vůči klasické měně stabilní. To znamená, že 1 Stable coin má hodnotu 1 fiat měny v závislosti, na kterou je fixován. Celé toto provázaní musí být transparetní, aby lidé měli důvěru, že je tato digitální měna podložena měnou reálnou. To v podstatě znamená, že Stable coiny musí mít nějakou centrální autoritu, tedy emitenta, který zajišťuje směnu mezi digitální měnou a klasickou fiat měnou. Funguje to tedy tak, že klasické fiat peníze uživatel pošle na účet emitenta, který mu na základě platby vyemituje dané množství digitální měny. Princip tohoto fungování je velmi podobný dluhopisům, jelikož uživatel půjčí klasickou fiat měnu emitentovi, který mu za to dá digitální měnu (dluhopis), ale není zde žáden úrok. Je to tedy forma chytrého kontraktu, kde se emitent zavazuje držet vložené prostředky na účtu, aby zajistil možnost okamžité směny zpět na klasické fiat peníze. Díky tomu lze pracovat doslova s klasickou fiat měnou na blockchainové technologii a využívat všechny výhody této technologie.

5.2.1 USDC - USD Coin

USD Coin je stable coin, za kterým stojí společnost Circle, Bitmain a Poloniex. Je to digitální měna vázaná na americký dollar. Využivá blockchain od Ethereum, tedy tokeny ERC-20, což je nejpoužívanější forma tokenů na Ethereum. Objem peněz v USDC ke dni 8.5.2020 je 708 000 000 $.

5.2.2 USDT - USD Tether

USD Tether je stable coin, opět vázaný na americký dollar. Za vznikem a zároveň emitentem je Bitfinex. USDT používá také ERC-20, ale také Omni protokol nad Bitcoinovým blockchainem. Uživatel si může vybrat, na které platformě chce USDT používat, rozdíly jsou především v poplatcích za transakce, respektivě rozdíl poplatků na Ethereum a Bitcoin blockchainu. Objem peněz v USDT je 7 850 000 000 $ k 8.5.2020.

USDT má však za sebou jeden velký skandál, kdy byl obviněn z manipulace celého kryptotrhu prostřednictvím emitování nepodložených USDT tokenů[28]. Díky tomu mohli Bitcoin nakupovat doslova zadarmo a zvyšovat tímto jeho hodnotu.

5.2.3 True USD

Kvůli problémům s transaparentností USDT vznikl projekt True USD. Jeho hlavním cílem bylo přinést transaparetnost a zamezit manipulacím a svévolné emitaci falešené měny. Opět využívá stejný princip fungování jako ostatní stabilní měny, ale vnáší větší míru transparentnosti. Projekt se stále vyvíjí a jeho cílem je vyřešit problém s centrálním prvkem, respektivě emitentem. Ve srovnání s USD a USDT je objem peněz v této měně malý, a to ke dni 2.5.2020 je 40 milionů dollarů.

5.3 Blockchainové knihovny

Dnes máme k dispozici mnoho opensource projektů, které umožňují jednoduše implementovat blockchain do svých projektů a potřeb. Často jsou to velice pokročilé projekty, na kterých pracují velké firmy a stovky lidí v komunitě.

5.3.1 Hyperledger

Hyperledger Fabric je nejznámějším open source řešení blockchainové technologie. Pomocí tohoto nástroje lze vytvořit projekt jak soukromý, ale také veřejný pro široké spektrum blockchain projektů. Za tímto nástrojem stojí Linux Foundation.

Na vývoji tohoto projektu spolupracují stovky firem a dobrovolníků. Mezi vývojáře, ale i uživatele této technologie patří velké světové firmy jako SAP, IBM či Huawei. Pro tyto firmy je to skvělý nástroj jak jednoduše a rychle implementovat blockchain do jejich organizace.

Tento nástroj patří momentálně mezi absolutní špičku v oblasti blockchainu, díky čemuž získává pozornost firem z celého světa. Pomocí tohoto nástroje velké banky jako J.P. Morgan, Deutsche Börse a další významné organizace nasazují technologii blockchain. Největší světová burza na WallStreet také plánuje nasazení tohoto projektu v blízke době.

5.3.2 Quorum

Tento projekt vychází z Ethereum. Přebírají většinu kódu právě od Ethereum a navíc přidávají časti, které se hodí především pro podnikové využití. Tento projekt cílí především na podniky a korporace, kterým tímto nabízí kompletní řešení pro přechod či nové služby na blockchainu.

Tento projekt si lze představit jako knihovnu pro vytváření blockchainu. Vzniká v partnerství s J.P.Morgan a Microsoftem. Existují i některé menší burzy, které prostřednictvím tohoto projektu implementovali nákup zlata prostřednitvím tokenů v blockchainu.

6 Vlastní implementace

6.1 Proč vlastní implementace

V této práci jsem zvolil cestu vlastní implementace, nikoliv použití již dostupné knihovny. Přináší to mnoho výhod, neboť takto mohu s blockchainem provádět jakékoliv operace a zároveň této problematice porozumím více do hloubky.

Cílem je vytvořit knihovnu, která umožní testovat různé vlastnosti blockchainu. Díky tomu, že implementace se bude zabývat základní verzí blockchainu, bude srozumitelná a každý si bude moci otestovat jeho vlastní experimenty. Mnohé dnešní open source projekty jsou příliš velké a komplikované a práce s nimi je daleko obtížnější než v případě vlastní jednoduché implementace.

6.2 Možnosti využití

Možnosti využití vlastní implementace spočívají především v seznámení se s blockchainem a jeho testováním. Nic však nebrání k realnému nasazení do jakéhokoliv projektu. Díky tomu, že tato implementace bude jednoduchá a přehledná, ji lze jednoduše rozšířit o další chování.

Má implementace v základní podobě bude fungovat jako kryptoměna, tedy blockchain 1.0, avšak nic nebrání k vytvoření i chytrých kontraktů nebo distribuovaného úložiště.

6.3 Návrh

Pro tvorbu této implementace jsem si vybral programovací jazyk Python. Mnohé projekty právě tento programovací jazyk používají, protože nabízí mnoho nástrojů, které tvorbu blockchainu ulehčují. Zároveň vyřeší problém přenositelnosti na jiné platformy.

Síťový přenos bude probíhat prostřednictvím soketů a data budou ve formě JSON, což umožní snadné vytvoření uzlu i v jiném programovacím jazyku.

Tato implementace bude blockchain 1.0 s možností rozšíření na libovolnou verzi. Blockchain 1.0 implementuje elektronický platební systém bez centrální autority, respektivě kryptoměnu, které v této práci budu říkat VSB Coin.

6.3.1 Uzly

V síti budu rozlišovat 4 uzly. Pro vytvoření plně funkčního blockchainu není více potřeba. Kromě DNS uzlu bude mít každý uloženo minimálně 5 sousedů, se kterými bude komunikovat. Uzly tedy budou následující:

- Plný uzel (Full node)

  Tento uzel bude klasickou obdobou plného uzlu jak bylo vysvětleno v části 3.4.2. Tento uzel bude v uchovávat celý blockchain a zároveň bude moct plnit funkci peněženky.

- Těžební uzel (Mining node)

Těžební uzel bude uchovávát celý blockchain, ale zároveň bude potvrzovat a vytvářet nové bloky. I tento uzel může fungovat jako peněženka. Vzhledem k tomu, že tato implementace bude v základu využívat nejčastěji používaný konsenzuální algoritmus důkaz o práci (PoW), tento uzel nesmí v síti chybět.

- Lehký uzel (Lightweight node)

  Tento uzel bude nejčastěji využívaný uzel, protože nevyžaduje žádné speciální výpočetní či prostorové nároky. Bude to klasická peněženka, která bude sloužit k odesílání a přijímání transakcí, ale také jako routingový uzel, který přeposílá jiné požadavky přes síť.

- DNS uzel

  Nový uzel se nějakým způsobem musí dozvědět, ke komu se připojit. Právě kvůli této skutečnosti bude v síti minimálně jeden DNS uzel, který bude udržovat seznam aktivních uzlů. Uzel bude mít fixní známou adresu, aby se nové uzly mohly dotazovat na ostatní uzly.

6.3.2 Adresy

Tato implementace bude využívat pro vytváření adres peněženek asymetrické šifrovací alagoritmy. Veřejný klíč bude sloužit jako adresa peněženky, respeketivě heš z veřejného klíče, a privátní klíč bude sloužit k podepisování transakcí. Každý uzel si bude moct vytvořit neomezené množství těchto dvojic klíčů a tím pádem i adres.

Záměrně neuvádím konkrétní algoritmy, které budou pro šifrování či hešování použity, neboť pro každou jednotlivou implementaci budou volitelné.

6.3.3 Zprávy

V této P2P síti bude probíhat komunikace, jak již bylo zmíněno, skrz sokety a prostřednictvím JSONu. Každý jeden síťový požadavek bude chápán jako určitá zpráva, která bude podle hlavičky rozpoznána. Každá tato zpráva má v sobě jednoznačný identifikátor, aby se zamezilo zacyklování a zahlacování sítě. V síti se tedy budou rozlišovat tyto zprávy:

- Zpráva GET_PEERS a GET_PEERS_ANSWER

  Zprávy s těmito hlavičkami slouží k nalezení sousedů, se kterými můžeme komunikovat. Tuto zprávu jsou schopné zpracovat všechny uzly a především uzel DNS řeší tyto zprávy při připojení nového uzlu do sítě. V požadavku na seznam uzlů musí uzel uvést informace o sobě a počet uzlů, které chce.

- Zpráva GET_BLOCK a GET_BLOCK_ANSWER

  Jak už je z názvu patrné, tyto zprávy zajištují bloky na vyžádání. Například v případě, že plný uzel bude nějaký čas offline a poté se opět připojí, může pomoci těchto zpráv zajistit

stažení bloků, které se vytvořili po dobu, kdy nebyl připojen. Zároveň umožňují uživateli nahlédnout do jakéhokoliv bloku.

- Zpráva GET_BALANCE a GET_BALANCE_ANSWER

  Tato zpráva slouží především pro uzly s aktivní peněženkou, které prostřednictvím této zprávy zjistí, jaký mají zůstatek na dané adrese.

- Zpráva GET_TRANSACTION a GET_TRANSACTION_ANSWER

  Tyto zprávy umožňují to stejné, jako GET_BLOCK, akorát s transakcemi. Tedy každý uzel si může prohlédnout libovolné transakce.

- Zpráva GET_BLOCKCHAIN a GET_BLOCKCHAIN_ANSWER

  Tuto zprávu využijí především nové plné uzly a těžaři. Prostřednictvím této zprávy dokáže uzel získat kompletní blockchain.

- Zpráva NEW_TRANSACTION

  Tato zpráva posílá informace o nové transakci. Zprávy putují až k těžařům, kteří tuto transakci poté zařadí do fronty čekající na potvrzení.

- Zpráva NEW_BLOCK

  Jakmile těžaři vytěží nový blok, tak prostřednictvím této zprávy oznamují jeho nalezení. Nový blok si poté ostatní zařadí do blockchainu, jestliže ho ještě nemají.

- Zpráva CONNECTED a CONNECTED_OK

  Touto zprávou dáva uzel najevo, že je aktivní. Ostatní uzly, kterým se takto ohlásí, mu poté budou přeposílát veškerou komunikaci. Druhý uzel mu na tuto zprávu odpoví a tímto se považuje spojení za navázané.

Samotná zpráva se skládá z těchto dat:

- IP adresa odesílatele
- Typ zprávy
- ID zprávy
- Odpověď na ID
- Data

6.3.4 Transakce

Transakce hrají v blockchainu, který slouží jako kryptoměna, velkou roli. V této iplementaci se bude transakce skládat z těchto položek:

- Časové razítko
- Adresa odesílatele
- Veřejný klíč odesílatele
- Adresa příjemce
- Suma
- Poplatek
- Zůstatek odesílatele po provedení transakce (Vyplňuje těžař při potvrzení)
- Zůstatek příjemce po provedení transakce (Vyplňuje těžař při potvrzení)
- Heš transakce / Identifikátor transakce
- Podpis této transakce

6.3.5 Bloky

Jak už bylo popsáno blockchain je řetěz bloků a blok je tedy základní stavební prvek. V mé implementaci budou bloky ukládat tyto informace:

- Časové razítko
- Výška bloku
- Těžař, který blok vytvořil
- Heš přechozího bloku
- Heš aktuálního bloku
- Nonce
- Pole transakcí

6.4 Funkčnost

V této další podkapitole popíši, jak celá tato implementace funguje. Aby celá síť mohla fungovat, musí být spuštěn DNS uzel. Je to první uzel a je nutností, mít ho spuštěň, aby se dal celý VSB Coin spustit. Důvod je jednoduchý, nové uzly by se neměly šanci dozvědět o ostatních uzlech v síti. Nejdříve je však potřeba nastavit jednotnou konfiguraci všech uzlů.

6.4.1 Konfigurace

Aby celý blockchain mohl správně fungovat, musí mít všechny uzly správnou konfiguraci. V této konfiguraci je nastaveno celé fungování VSB Coin. Pokud by každý uzel měl jinou konfiguraci, mohlo by v závislosti na rozdílech v této konfiguraci docházet k forkům. Z čeho se tedy tato konfigurace skládá:

- Volba algoritmu pro asymetrickou kryptografii
- Volba hešovací funkce pro vytváření adresy
- Volba hešovací funkce pro heš transakce
- Volba hešovací funkce pro heš bloku
- Pravidla pro složitost těžby
- Maximální počet transakcí v bloku

6.4.2 Připojení k síti

V této implementaci existují 2 způsoby, jakými se dokáže uzel připojit do sítě. Buď získá informace o dalších uzlech z DNS uzlu nebo již tento seznám má. Seznam těchto uzlů lze zapsat do zdrojového kódu nebo může být uložen z doby, kdy byl spuštěn naposledy.

Jakmile se tedy uzel zapne a získá seznam sousedů nebo ho již má, všem těmto uzlům pošle zprávu CONNECTED. Po tomto úvodním procesu je uzel připraven k fungování.

6.4.3 Vytvoření adresy

Pokud je uzel úspěšně připojen k síti a navázal spojení, nemusí nic dělat a může sloužit jako pouhý přeposílací uzel. Avšak nejčastěji bude pokračovat vytvořením adresy, pokud ji stále nemá.

Uzel vytvoří dvojici klíčů podle zvoleného algoritmu a z veřejného klíče následně prostřednictvím hešovací funkce pro vytváření adresy vypočte heš, který bude sloužit jako adresa VSB Coin peněženky.

6.4.4 Genesis blok

První těžební uzel vytvoří Genesis blok, tedy speciální blok, za který získá první odměnu. Tento blok vytváří těžař speciální funkcí, protože se jedná o mimořádný blok, který nemá referenci na předchozí blok. Poté již může samotný těžař, ale i ostatní těžaři vytvářet bloky běžným způsobem.

Bloky se vytváří i v případě, že v síti nejsou žádné transakce. Funguje to takto i u většiny ostatních kryptoměn. Nedávno se toto stalo právě u Bitcoinu, kdy byl vytěžen prázdný blok.

6.4.5 Vytvoření zprávy

Aby se informace o nových blocích, transakcích a o všem dalším dostali k jiným uzlům, je třeba vytvořit a odeslat zprávu. Vytvoření nové zprávy probíhá takto:

1. Uzel vytvoří novou zprávu
2. Vyplní svou IP adresu a pomocí hešovací funkce vytvoří ID zprávy z časového razítka a jeho IP

6.4.6 Odeslání transakce

Jakmile má uživatel k dispozici nějaké prostředky, což může zajistit zprávou GET_BALANCE, může poslat tyto prostředky jinému uživateli. Na začátku VSB Coin budou moci odesílat první platby těžaři, neboť běžné uzly nebudou mít možnost měnu získat jinak, než přijetím platby.

V případě, že uživatel chce platbu odeslat, potřebuje znát pouze adresu příjemce a sumu, kterou odesílá. Avšak je nutností zadat velikost poplatku, který obdrží těžař za zařazení této trasakce do bloku. Teoreticky může vytvořit i transakci s vyšší sumou než má k dispozici, ale jeho transakce nebude potvrzená dříve, než bude mít potřebné prostředky k dispozici. Postup vytvoření a odeslání nové transakce je tedy tento:

1. Odesílatel zadá adresu příjemce, sumu a poplatek.
2. Poté se začne vytářet transakce, zapíše se aktuální čas, adresa odesílatele, adresa příjemce, suma a velikost poplatku.
3. Na základě těchto informací se vytvoří heš dle algoritmu v konfiguraci.
4. Tento heš se podepíše soukromým klíčem odesílatele a připojí se k transakci.
5. Nakonec se přidá veřejný klíč odesílatele a transakce se odešle jako zpráva všem sousedním uzlům.

6.4.7 Zpracování příchozí zprávy

V závislosti na tom, jaký typ uzlu obdrží zprávu, proved uzel určité operace. Jedná-li se o lehký uzel, uloží si ID zprávy a zprávu odešle dále všem svým sousedům. Je potřeba si uložit ID, aby následně některý ze sousedů neposlal stejnou zprávu a uzel by ji znova přeposlal. Pokud zpráva nese informace o novém bloku, uzel se podívá, jestli náhodou v novém bloku není transakce, ve které se vyskytuje jeho adresa a to jak na straně odesílatele, tak na straně příjemce. Pokud takovou transakci najde, aktualizuje svůj zůstatek. Tento postup platí pro všechny uzly. V případě, že uzel obdrží GET_PEERS, podívá se na adresu odesílatele, projde své uložené sousedy a následně mu na tuto zprávu odpoví. V podstatě uzly odpovídají vždy, pokud znají odpověď na danou zprávu, v opačném případě pouze zprávy přeposílají.

6.4.8 Vytvoření nového bloku a potvrzení transakce

Vytváření nového bloku je nejdůležitější část implementace, protože bez správně vytvořených bloků a správně potvrzených transakcí nemůže blockchain existovat. Tento proces provádí pouze těžební uzel. Jakmile těžař chce začít tvořit/těžit nový blok, podívá se do svého seznamu nepotvrzených transakcí. Podle jeho preferencí vybere určité platby a poté následuje tento postup:

1. Vybrané transakce nejprve zkontroluje jestli jsou validní. Tento proces spočívá v tom, že se těžař podívá do blockchainu, jestli odesílatel má dané prostředky, které chce poslat. Poté ještě zkontroluje, jestli jsou zadané adresy validní, ale nekontroluje, jestli daná adresa existuje.

2. Transakce, které prošly validací jsou zařazeny do nového bloku. Těžař sečte všechny poplatky z těchto transakcí.

3. Poté přidá těžař speciální transakci, které se říká coinbase transakce. Tato transakce nemá odesílatele, ale pouze příjemce. V této implementaci pouze nastavím adresu odesílatele jako VSB. Tato transakce bude mít hodnotu jako součet poplatků za transakce v bloku + odměnu za vytvoření nového bloku. Odměna za vytvoření nového bloku se bude řídit dle konfigurace.

4. Jakmile těžař připraví všechny transakce včetně coinbase, přidá do bloku identifikátor předchozího bloku, jméno těžaře a výšku bloku.

5. Na základě všech informací v bloku začne generovat nonce. Pro každou nonci, kterou vygeneruje a následně přidá do bloku, musí vypočítat z daného bloku heš pomocí hešovací funkce. Jakmile daný heš splní podmínku, kterou se určuje aktuální složitost, těžař uloží odpovídající nonci, přidá časové razítko a tento heš přidá do bloku.

6. Poté je daný blok vytvořen a těžař musí tento blok poslad co nejrychleji mezi ostatní uzly, ať ostatní těžaři netěží blok o stejné výšce znova, ale navazují na tento blok.

7 Otestování funkčnosti a experimenty s VSB Coin

Nyní je potřeba tuto implementaci otestovat. Aby se implementace dala otestovat, je potřeba mít několik uzlů. Nejméně z každého uzlu jeden, ale reálně je potřeba více. Pro prvotní testování zvolím deset uzlů. Deset uzlů znamená, že potřebuji nejlépe 10 počítačů. Proto jsem pro potřeby testování a experimentování zvolil přístup virtuálních počítačů.

7.1 Testovací síť

Pomocí aplikace VirtualBox vytvořím virtuální síť. Následně do této sítě přidám deset uzlů. Všechny počítače mají stejný operační systém a to Linux Debian. Tyto systémy jsou na všech uzlech úplně stejné, všechny uzly vychází z jednoho obrazu. Každý počítač pro přehlednost pojmenuji podle toho, jaký typ uzlu bude provozovat.

DNS uzel musí mít pevně danou a neměnnou IP adresu, aby se ostatní uzly dokázaly k němu připojit. Ostatní uzly mohou mít dynamickou IP adresu, protože v případě potřeby se dokáží k ostatním uzlům připojit skrz DNS uzel. Na obrázku 19 je vidět struktura mé testovací virtuální sítě.

Testovací síť bude mít toto složení uzlů:

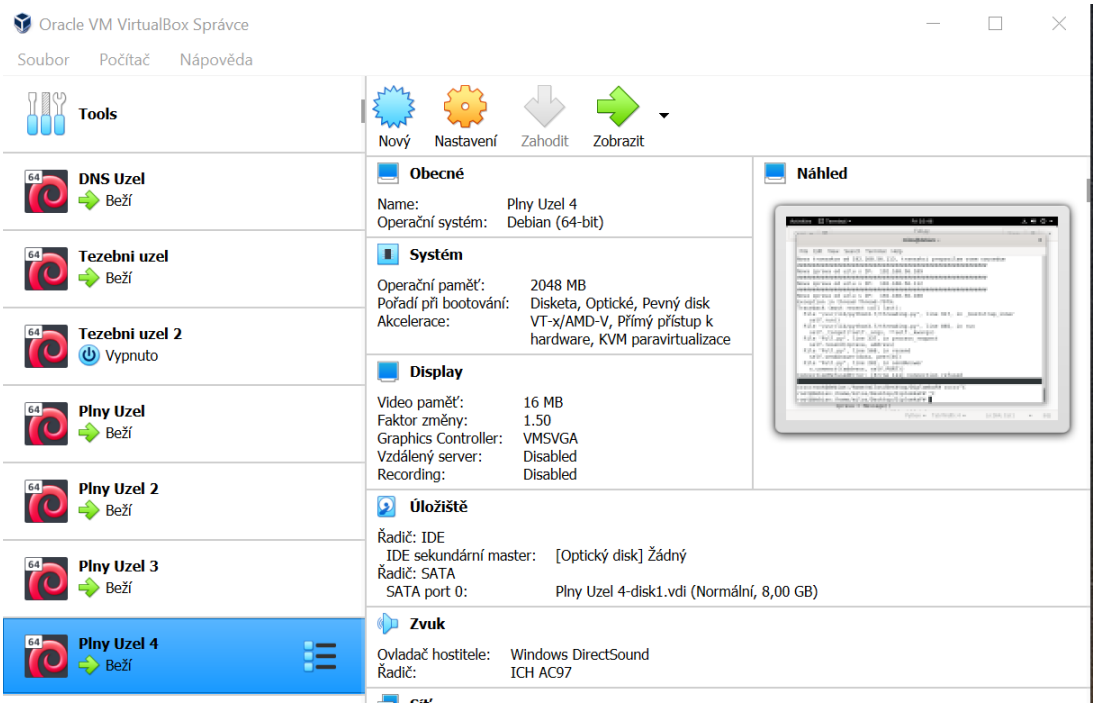
- 1 DNS uzel
- 2 Těžební uzly
- 2 Plné uzly
- 5 Lehké uzly

Důvodem pro toto rozložení uzlů bylo především to, abych dokázal otestovat práci více než jednoho těžaře současně. Dva plné uzly jsou pro ověření správné distribuce nových bloků a jejich správného navazování. Lehké uzly budou vytvářet provoz.

7.2 Spuštění testovací sítě

První spuštění sítě vyžaduje určité kroky, které se musí provést manuálně. Nejprve se jedná o spuštění DNS uzlu, který zajistí konektivitu pro další uzly. Jakmile běží DNS uzel, do sítě připojím těžební uzel, který začne těžit nové bloky. Tento první těžební uzel má nárok na odměnu za genesis blok. Blok s výškou 2 již poté navazuje standartně na genesis blok.

Nyní se do sítě mohou připojit ostatní uzly a započít komunikace. Problémem je, že při startu blockchainu mají danou měnu pouze těžaři. Pro otestování sítě jsem musel vymyslet, jakým způsobem odesílat platby, abych vytvořil reálný provoz. Transakce lze odesílat ručně, ale pro potřeby testování a získání statistik je to neefektivní. Pro potřeby testování jsem nastavil každému uzlu automatické rozesílání plateb na náhodně vybrané adresy ostatních uzlů.



Obrázek 19: VirtualBox testovací síť

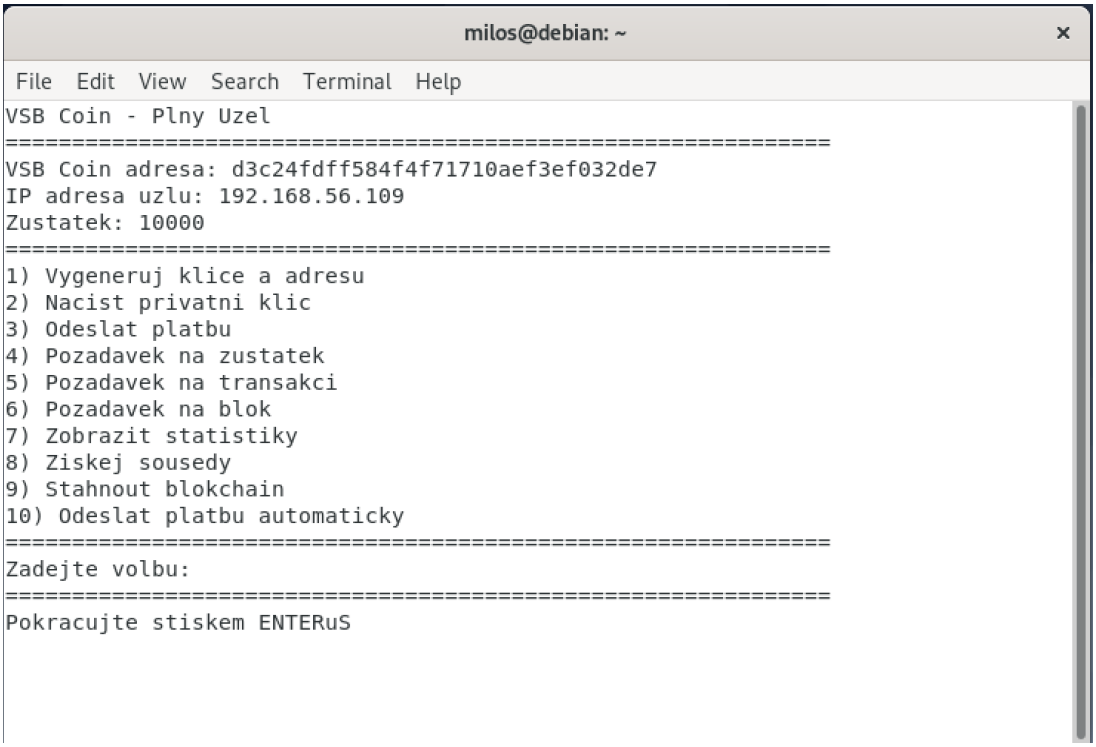
V coinbase transakci genesis bloku je nastavena mimořádně velké odměna. To umožní, aby se dalo z peněženky těžaře, který tuto transakci vytvořil mohl přeposlat částku na další uzly, které budou následně generovat provoz. Pro účely testování je odměna za genesis nastavena na 10 000 VSB Coin. Na uzlech sloužicí pro generování provozu vytvořím peněženky z důvodu získání VSB Coin adres a tyto adresy vložím do pole podle, kterého se bude vytvářet provoz. Na každou z těchto adres pošlu 2000 VSB Coin a spustím generování provoozu.

Vlivem testování na virtuálních počítačích a zároveň ve virtuální siti dochází k velmi nízkým odezvám sítě. Pro účely testování to nevadí, protože to zajistí velmi podobné testovací podmínky pro různé konfigurace. Každý uzel má k dispozici 2 GB RAM, 1 virtuální procesor a 8 GB paměti. Hostitelský počítač VirtualBoxu má k dispozici procesor AMD Ryzen 9 3900X s 12 jádry a 128 GB RAM, díky čemuž můžu provádět testování i s více uzly a velkým provozem.

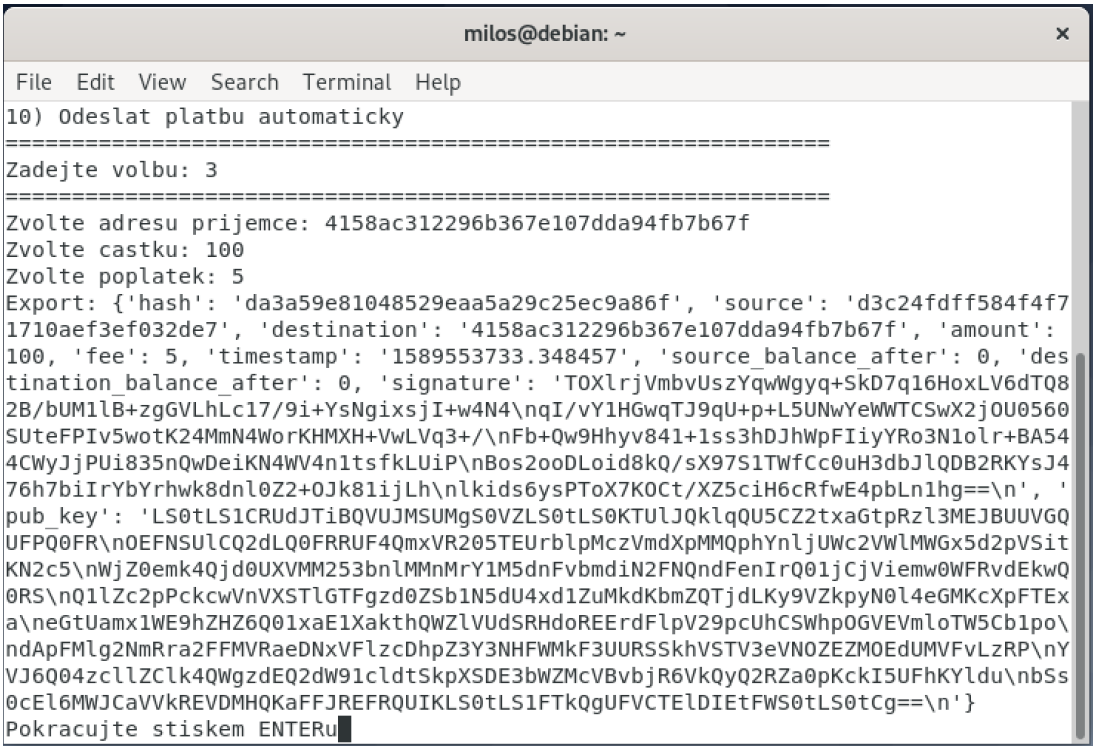
Na obrázcích 20 až 22 lze vidět podobu hotové implementace ve virtuálním stroji. Obrázek 20 znázorňuje podobu plného uzlu v síti a jeho možnosti interakce se sítí. Uzel má vytvořenou VSB Coin adresu, na které má 10000 jednotek této měny.

Obrázek 21 znázorňuje použití plného uzlu při vytvoření s odesláním transakce. Na obrázku je vidět zadaná adresa, kam se měna posílá společně s částkou a poplatkem. Pro kontrolu uzel ukáže údaje z této transakce v podobě, jak se následně pošlou do sítě. Lze vidět, že se vypočítal heš transakce a zaznamenalo se časové razítko. Transakce také obsahuje řetězcovou podobu serializovaného veřejného klíče a podpisu dané transakce pro ověřené pravosti transakce.

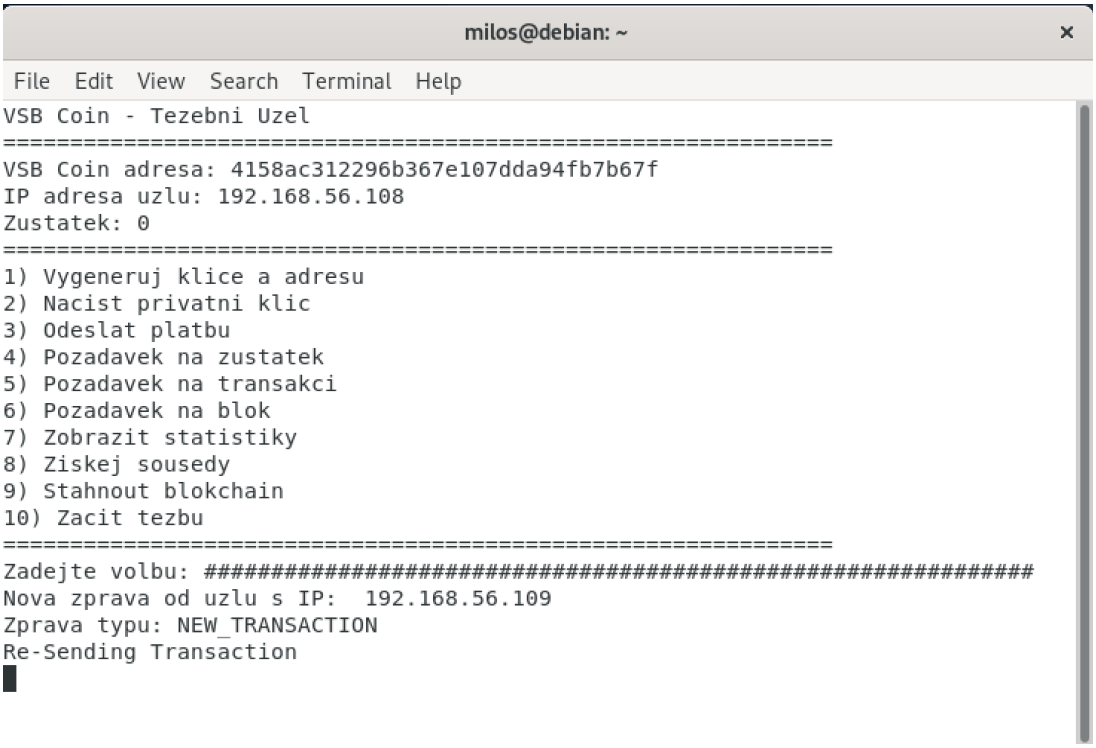
Jak to vypadá po obdržení nové zprávy ze sítě, je vidět na obrázku 22. Na snímku je za-



Obrázek 20: Snímek obrazovky plného uzlu



Obrázek 21: Snímek obrazovky plného uzlu při odeslání transakce



Obrázek 22: Snímek obrazovky těžebního uzlu po obdržení transakce

chycen těžební uzel se všemi jeho možnostmi v momentě, kdy k němu ze sítě dorazila zpráva o nové transakci, která se odeslala v předchozím obrázku. Zároveň je vidět text "Re-Sending Transaction", který říká, že se tato zpráva s novou transakcí přeposílá dalším uzlům v síti, které nejsou v přímém spojení s plným uzlem z předchozího obrázku.

7.3 Příprava konfigurací pro testování

Postupně provedu testování na různých konfiguracích protokolu. Výsledky testování se pokusím vysvětlit. Z výsledku se budu snažit nalézt optimální nastavení sítě, kdy nebude vznikat v síti velká fronta nepotvrzených transakcí, zároveň se nebudou vytvářet příliš velké bloky, které by poté bylo náročné distribuovat po síti.

Složitost určuje, jakou nonci těžař musí nalézt, aby zajistila, že výstup z hešovací funkce bloku bude začínat X stejnými znaky. To, který znak to má být určuje nastavení v konfiguraci. Odměna za nalezení této nonce, respektivě za vytvoření nového bloku je Y VSB Coin + poplatky. Složitost 1 platí pro bloky s výškou menší než Z. Složitost může být rostoucí (tabulka 2) a konstatní (tabulka 3). V případě konstatní složitosti pouze klesá odměna pro těžaře, ten přístup je vhodný především pro testovací účely.

Tabulka 4 obsahuje konfiguraci pouze s parametry, které zásadně ovlivňují výkonnost sítě. Ostatní parametry jsou spíše pro budoucí experimenty. Všechny tyto konfigurace otestuji na stejné síti a se stejným natavením generování provozu, které je popsáno v tabulce 5. Zároveň

Z (výška bloku)	10	20	30	40	50	500
X (počáteční znaky)	2	3	4	5	6	7
Y (odměna)	100	50	25	12.5	6.25	3.125

Tabulka 2: Rostoucí složitost

Z (výška bloku)	10	20	30	40	50	500
X (počáteční znaky)	4	4	4	4	4	4
Y (odměna)	100	50	25	12.5	6.25	3.125

Tabulka 3: Konstantní složitost

Konfigurace	1	2	3	4	5	6
Hešovaci funkce bloků	md5	md5	md5	sha256	sha256	sha256
Maximální počet transakcí v bloku	10	25	50	10	25	50

Tabulka 4: Nastavení konfiguraci

Interval pro vytvoření transakce		Částka		Poplatek	
Od	Do	Od	Do	Od	Do
1	30	5	25	1	5

Tabulka 5: Pravidla pro generování transakci

Výška	Hash	Předchozí hash	Nonce
12	aaaa23844c83f16e40a9b72b59703055	aaaa6c7a6a14d87dd0cd1168351d670b	149147
13	aaaa35a3bc46e18558484e7bd0d8db55	aaaa23844c83f16e40a9b72b59703055	60555
14	aaaa4ad084ec883453bcbe62af9ab601	aaaa35a3bc46e18558484e7bd0d8db55	46990

Tabulka 6: Výběr z výstupního souboru bloků

Odesílatel	Příjemce	Částka	Poplatek	O. Zůstatek	P. Zůstatek	Blok
d3c24....2de7	d9a8....a687	4	3	2452	2506	40
VSB TUO	4158....b67f	9.25	0	0	4221.5	40
d3c2....2de7	c27a....cb33	4	2	2446	2504	41

Tabulka 7: Výběr z výstupního souboru transakcí

horní limit intervalu vytvoření transakce se v čase snižuje, abych nasimuloval nové uzly v síti, které generují nový provoz. To by mělo zajistit, že provoz v síti bude v čase růst a bude testování bude odpovídat realitě.

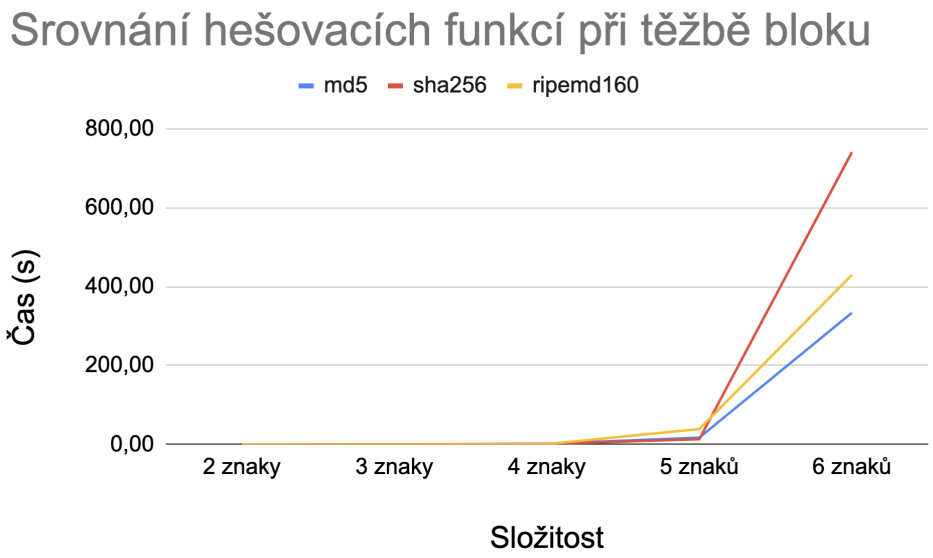
To by mělo zajistit objektivní hodnocení výkonnosti sítě. Každé testování zároveň provedu na rostoucí i konstatní složitosti. Zaměřím se vždy pouze na prvních 50 bloků. Po vytvoření 50 bloků se automaticky vyexportují bloky s transakcemi do souboru.

7.4 Testování

Podle výše popsaných konfigurací začnu testovat blockchain. Nejprve, ale musím ověřit správnost vytváření bloků, validaci transakcí a přepočty zůstatků. Správně vytvořený blok musí obsahovat správnou referenci na předchozí blok. V tabulce 6, která je výběrem z výstupního souboru lze vidět, že bloky na sebe správně navazují.

V tabulce 7 je vidět několik zpracovaných transakcí. Jednou z nich, kde odesílatel je VSB TUO, je transakce coinbase, tedy odměna těžaři za vytvoření daného bloku. Dle složitosti měl dostat 6.25, ale obdržel 9.25 a to díky poplatku za transakce v bloku. V bloku 40 byly pouze 2 transakce, z toho jedna coinbase a jedna normální s poplatkem 3. To je důvod proč těžař získal 9.25 VSB Coin. Taky jde v této tabulce vidět, že odesílateli "d3c24....2de7"bylo správně odečteno 6 VSB Coin, z čehož 4 šly na adresu "c27a....cb33"a zbytek šel těžaří jako odměna za zařazení této transakce do bloku.

Na obrázku 23 a v tabulce 8 lze vidět jak dlouho trvá v průměru nalézt správnou nonci pro blok při složitosti N znaků. Do složitosti o počtu 4 znaků jsou rozdíly zanedbatelné, ale již u 5 znaků se projeví zpomalení hešovací funkce ripemd160. U složitosti 6 znaků se situace mění a hešovací funkce sha256 je nejpomalejší. Pro účely testování vlastnosti blockchainu VSB Coin jsou tyto rozdíly zanedbatelné, protože na složitosti 6 a více znaků neprovadím testy. Při reálném nasezení by však byla nejvhodnější funkce sha256 a to z bezpečnosti (md5 již není považován



Obrázek 23: Srovnání rychlostí hešovacích funkcí

Počet znaků	md5	sha256	ripemd160
2	0.02	0.04	0.01
3	0.22	0.19	0.22
4	2.15	1.50	1.26
5	17.59	13.45	39.29
6	333.52	740.38	429.52

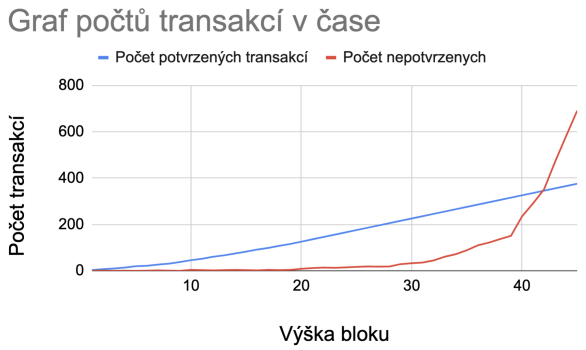
Tabulka 8: Srovnání rychlostí hešovacích funkcí. Hodnoty jsou uvedeny v sekundách

za bezpečný). Z naměřených hodnot lze usoudit, jak bude klesat propustnost sítě s rostoucí složitostí.

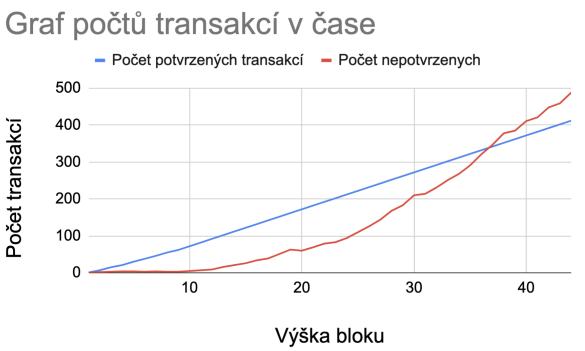
Nyní tuto vlastnost otestuji na reálné síti. Na základě srovnání rychlostí hešovacích algoritmů pro nalezení nonce daného bloku, budu testování provádět pouze na funkci md5. Podle tabulky 4 jsem postupně otestoval konfiguraci 1, 2 a 3. Dané konfigurace jsem otestoval jak na rostoucí složitosti, tak také na konstatní složitosti podle tabulek 2 a 3.

Na obrázku 24 je vidět konfigurace s maximálně 10 transakcemi v bloku. Obrázek 21(a) ukazuje, že v určitém čase počet nepotvrzených transakcí převýší počet transakcí potvrzených a dále exponenciálně stoupá. Z tohoto lze usoudit, že tato konfigurace není vhodná pro tuto síť, neboť nepotvrzené transakce budou postupně čekat na potvrzení stále delší dobu. Stejný případ lze vidět i u konstantní složitosti, kde však tento nárůst nepotvrzených transakcí neroste tak razantně. Tato konfigurace se hodí pro případ s nízkou složitostí těžby nebo s nízkým počtem transakcí, například systém pro katastr nemovitostí, kdy změny u nemovitostí nejsou tak časté.

Obrázek 25 popisuje konfiguraci s maximálně 25 transakcemi v bloku. Ve srovnání s předchozím případem je vidět, že navýšení maximálního počtu transakcí v bloku způsobilo vyšší

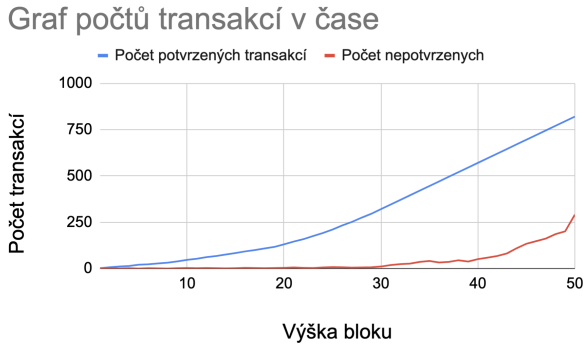


(a) Rostoucí složitost

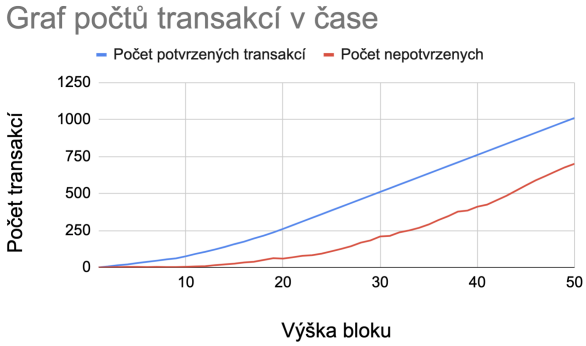


(b) Konstatní složitost

Obrázek 24: Konfigurace s 10 transakcemi v bloku



(a) Rostoucí složitost



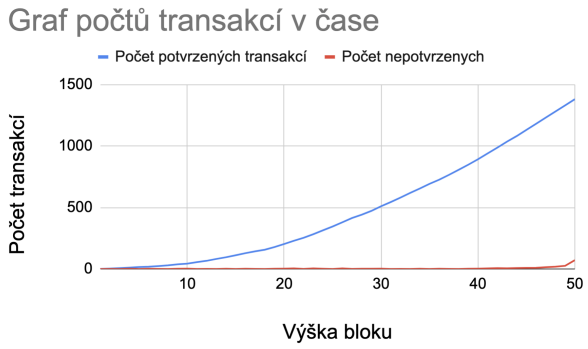
(b) Konstatní složitost

Obrázek 25: Konfigurace s 25 transakcemi v bloku

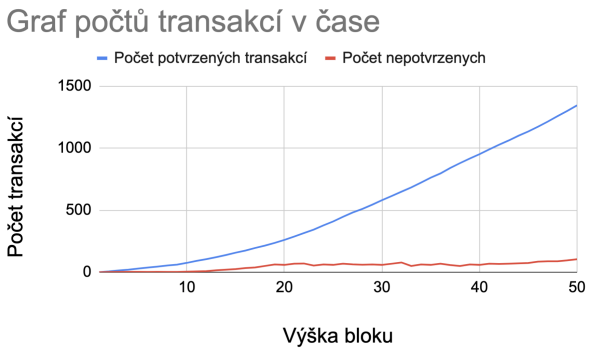
propustnost sítě, ale pokud by provoz v síti pokračoval dále, došlo by pravděpodobně ke stejnému případu jako na obrázku 21, protože lze vidět, že u posledních 10 bloků začal počet nepotvrzených transakcí opět stoupat. V případě konstantní složitosti se sice počet nepotvrzených transakcí drží pod počtem potvrzených transakcí, ale i tak počet těchto nepotvrzených transakcí stále roste a nelze vidět důvod, proč by se to mělo změnit. Proto je toto řešení pro provoz, který testovací síť generuje, stále nedostačující.

Poslední konfigurace s 50 transakcemi v bloku je na obrázku 26. Tato konfigurace zvládla testovací provoz do 50. bloku bez problému a udržovala počet nepotvrzených transakcí skoro konstantní. Na úplný závěr je vidět malý nárůst nepotvrzených transakcí. V případě konstantní složitosti síť opět provoz zvládla bez problému. Počet nepotvrzených transakcí se pohybal okolo stovky, z čehož můžeme usoudit, že nová transakce bude následně potvrzena v rámci dvou až tří dalších bloků.

Z tohoto srovnání se zdá, že vyšší počet transakcí v bloku je ideální řešení, avšak toto není úplně pravda, jelikož jsem testoval ve virtuální sítí s nízkou odezvou a data neproudila skrz



(a) Rostoucí složitost



(b) Konstatní složitost

Obrázek 26: Konfigurace s 50 transakcemi v bloku

internetovou síť. Vyšší množství transakcí v bloku zvyšuje datovou náročnost distribuce nově vytěžených bloků v síti. Proto je třeba volbu maximálního počtu transakcí v bloku vždy zvážit podle využtí dané blockchainové aplikace, ale také brát v potaz rychlost připojení do sítě.

V dalším experimentu jsem do sítě přidal 40 obyčejných uzlů a 2 těžební uzly. Obyčejné uzly generovaly minimální provoz a sloužily pouze pro otestování toho, jak se chová distrbuce zpráv v síti. Z následného pozorování jsem zjistil, že se zde vyskytuje fenomén malého světa, který popisuje, že aby se zpráva dostala z jednoho konce sítě na druhý, stačí mu poměrně malý počet přeskoků v síti. V tomto případě jsem žádal síť o stažení blockchainu a v průměru stačily 3 přeposlání zprávy.

8 Závěr

Cílem práce bylo vytvořit framework pro testování blockchainové technologie. Tohoto cíle se podařilo dosáhnout za použití virtuálních počítačů, virtuální sitě a vlastní implementace blockchainu. Cílem bylo také otestovat tuto implementaci a návrhnout postup při testování blockchainových aplikací.

Vytvoření základního blockchainového frameworku pro testování vlastního blockchainu se povedlo, základní funkčnost je hotová, ale při práci jsme se potýkal s několika problémy při tvorbě. Tato implementace zvládá fungovat jako kryptoměna, uživatelé si mohou mezi sebou odesílat transakci, mohou stahovat jednotlivé transakce, bloky či celý blockchain. Jednotlivé uzly v síti dokáži mezi sebou komunikovat v síti pomocí mnou navrženého protokolu a celý systém dokáže fungovat bez centrální autority. Jediným centrálním prvkem je DNS uzel, který není nutno použít, pokud uživatel získá adresy uzlů jinou cestou, například manuálním zapsáním do kódu. Ověřil jsem, že transakce jsou správně zpracovány a bloky na sebe správně navazují.

Naměřené rychlosti při těžbě bloků klesají exponenciálně s rostoucí složitostí a narůstá počet nepotvrzených transakcí, díky tomu klesá propustnost celé sítě. Ukazuje se tedy, že algoritmmus PoW není efektivní i přesto, že ho využívá drtiva většina všech kryptoměn. Nutí těžební uzly, aby stále navyšovali svůj výpočetní výkon, aby měli šanci nalézt správnou nonci jako první. To zvyšuje energetickou náročnost a výpočetní výkon je z pohledu uživatele využíván neefektivně. Hlavním důvodem proč většina projektů využívá tento algoritmus je bezpečnost, neboť s rostoucí složitostí roste i náročnost podvržení blockchainu. Avšak otázka problému neefektivity tohoto algoritmu zůstává otevřená a je zde velký prostor pro nové konsenzuální algoritmy, které vyřešení problém nefektivity a plýtvání výkonu.

Literatura

1. *Bitcoin: A Peer-to-Peer Electronic Cash System* [online] [cit. 2020-02-24]. Dostupné z: https://bitcoin.org/bitcoin.pdf.
2. *New Benchmark Supports Claims of '10,000 TPS' Blockchain* [online] [cit. 2020-02-24]. Dostupné z: https://hackernoon.com/new-benchmark-supports-claims-of-10-000-tps-blockchain-2bc8db0b98b4:.
3. THAKKAR, P.; NATHAN, S.; VISWANATHAN, B. Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform. In: *2018 IEEE 26 th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems(MASCOTS)*. 2018, s. 264–276.
4. DINH, Tien Tuan Anh; WANG, Ji; CHEN, Gang; LIU, Rui; OOI, Beng Chin; TAN, Kian - Lee. *BLOCKBENCH: A Framework for Analyzing Private Blockchains*. 2017. Dostupné z arXiv: 1703.04057 [cs.DB].
5. BALIGA, Arati; SUBHOD, I; KAMAT, Pandurang; CHATTERJEE, Siddhartha. *Performance Evaluation of the Quorum Blockchain Platform*. 2018. Dostupné z arXiv: 1809.03421 [cs.CR].
6. *A Next-Generation Smart Contract and Decentralized Application Platform* [online] [cit. 2020-02-25]. Dostupné z: https://github.com/ethereum/wiki/wiki/White-Paper.
7. *Blockchain Testing: Tools, Techniques, and Considerations* [online] [cit. 2020-02-25]. Dostupné z: https://pdfs.semanticscholar.org/b46a/0f59ddd3128169727faac572a0286585ed34.pdf.
8. CHEN, Si; ZHANG, Jinyu; SHI, Rui; YAN, Jiaqi; KE, Qing. A Comparative Testing on Performance of Blockchain and Relational Database: Foundation for Applying Smart Technology into Current Business Systems. In: 2018-01, s. 21–34. ISBN 978 - 3 - 319 - 91124 - 3. Dostupné z DOI: 10.1007/978-3-319-91125-0_2.
9. CHEN, Chen; QI, Zhuyun; LIU, Yirui; LEI, Kai. Using Virtualization for Blockchain Testing. In: 2018-01, s. 289–299. ISBN 978 - 3 - 319 - 73829 - 1. Dostupné z DOI: 10.1007/978-3-319-73830-7_29.
10. DWIVEDI, Ashutosh Dhar; SRIVASTAVA, Gautam; DHAR, Shalini; SINGH, Rajani. A Decentralized Privacy-Preserving Healthcare Blockchain for IoT. *Sensors*. 2019, roč. 19, č. 2. ISSN 1424-8220. Dostupné z DOI: 10.3390/s19020326.
11. SEOK, Byoungjin; PARK, Jinseong; PARK, Jong Hyuk. A Lightweight Hash-Based Blockchain Architecture for Industrial IoT. *Applied Sciences*. 2019, roč. 9, č. 18. ISSN 2076-3417. Dostupné z DOI: 10.3390/app9183740.

12. ANDONI, Merlinda; ROBU, Valentin; FLYNN, David; ABRAM, Simone; GEACH, Dale; JENKINS, David; MCCALLUM, Peter; PEACOCK, Andrew. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renewable and Sustainable Energy Reviews*. 2019, roč. 100, s. 143–174. ISSN 1364-0321. Dostupné z DOI: https://doi.org/10.1016/j.rser.2018.10.014.

13. *Performance and Scalability of Blockchain Networks and Smart Contracts* [online] [cit. 2020-02-27]. Dostupné z: https://umu.diva-portal.org/smash/get/diva2:1111497/FULLTEXT01.pdf.

14. *How to Time-Stamp a Digital Document* [online] [cit. 2020-02-28]. Dostupné z: https://www.anf.es/pdf/Haber_Stornetta.pdf.

15. *Ouroboros: A Provably Secure Proof-of-Stake Blockchain Protocol* [online] [cit. 2020-02-29]. Dostupné z: https://whitepaperdatabase.com/cardano-ada-whitepaper/.

16. *Monero* [online] [cit. 2020-05-08]. Dostupné z: https://github.com/monero-project/research-lab/blob/master/whitepaper/whitepaper.pdf.

17. *Eclipse Attacks on Bitcoin's Peer-to-Peer Network* [online] [cit. 2020-05-08]. Dostupné z: https://eprint.iacr.org/2015/263.pdf.

18. MOHAISEN, Aziz; KIM, Joongheon. The Sybil Attacks and Defenses: A Survey. *The Smart Computing Review*. 2013-12, roč. 3. Dostupné z DOI: 10.6029/smartcr.2013.06.009.

19. YE, Congcong; LI, Guoqiang; CAI, Hongming; GU, Yonggen; FUKUDA, Akira. Analysis of Security in Blockchain: Case Study in 51%-Attack Detecting. 2018-09, s. 15–24. Dostupné z DOI: 10.1109/DSA.2018.00015.

20. *Swarm* [online] [cit. 2020-05-08]. Dostupné z: https://readthedocs.org/projects/swarm-guide/downloads/pdf/latest/.

21. *Storj: A Decentralized Cloud Storage Network Framework* [online] [cit. 2020-05-08]. Dostupné z: https://storj.io/storj.pdf.

22. STEICHEN, Mathis; FIZ PONTIVEROS, Beltran; NORVILL, Robert; SHBAIR, Wazen; STATE, Radu. Blockchain-Based, Decentralized Access Control for IPFS. In: 2018-07. Dostupné z DOI: 10.1109/Cybermatics_2018.2018.00253.

23. *Hedera: A Public Hashgraph Network Governing Council* [online] [cit. 2020-05-08]. Dostupné z: https://www.hedera.com/hh-whitepaper-v2.0-17Sep19.pdf.

24. *The Tangle* [online] [cit. 2020-05-08]. Dostupné z: https://assets.ctfassets.net/r1dr6vzfxhev/2t4uxvsIqk0EUau6g2sw0g/45eae33637ca92f85dd9f4a3a218e1ec/iota1_4_3.pdf.

25. *Lite Coin White paper* [online] [cit. 2020-05-08]. Dostupné z: http://zioncoins.co.uk/wp-content/uploads/2015/06/Lite-Coin-Whitepaper.pdf.

26. *A NEXT GENERATION SMART CONTRACT DECENTRALIZED APPLICATION PLATFORM* [online] [cit. 2020-05-08]. Dostupné z: https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf.

27. *Cardano Introduction* [online] [cit. 2020-05-08]. Dostupné z: https://docs.cardano.org/introduction/.

28. *Bitfinex - Tether Lawsuit* [online] [cit. 2020-05-08]. Dostupné z: https://www.scribd.com/document/442403565/SDNY-Complaint.